DELITOS CONTRA LA SEGURIDAD INFORMÁTICA

Acceso ilícito
Atentados contra la integridad y disponibilidad
de datos y sistemas informáticos
Interceptación ilícita de datos informáticos
Abuso de dispositivos informáticos

Ricardo N. Elías Puelles
Profesor en la Pontificia Universidad Católica del Perú

DELITOS CONTRA LA SEGURIDAD INFORMÁTICA

ACCESO ILÍCITO • ATENTADOS CONTRA LA INTEGRIDAD Y DISPONIBILIDAD DE DATOS Y SISTEMAS INFORMÁTICOS • INTERCEPTACIÓN ILÍCITA DE DATOS INFORMÁTICOS • ABUSO DE DISPOSITIVOS INFORMÁTICOS

Prólogo de
Juan Carlos Ortiz Pradillo
Profesor en la Universidad Complutense de Madrid

Instituto Pacífico

INSTITUTO
PACÍFICO

DELITOS CONTRA LA SEGURIDAD INFORMÁTICA
Acceso ilícito. Atentados contra la integridad y disponibilidad de datos y sistemas informáticos. Interceptación ilícita de datos informáticos. Abuso de dispositivos informáticos.

Autor:
© Ricardo N. Elías Puelles, 2025

Primera edición - Julio 2025

Logo Actualidad Penal
El logo se encuentra en la carátula ya que el libro pertenece a la suscripción de la revista Actualidad Penal

Copyright 2025
Instituto Pacífico S.A.C.

Diseño, diagramación y montaje:
Luis Ruiz Martínez
Nora Villaverde Soldevilla

Edición a cargo de:
Instituto Pacífico S.A.C.-2025
Jr. Castrovirreyna 224, Breña, Lima, Perú
Central: 619-3700
E-mail: preprensa@institutopacifico.pe

Tiraje: 4500 ejemplares

ISBN : 978-612-322-615-2
Hecho el Depósito Legal en la Biblioteca Nacional del Perú N.°: 2025-07756

Impresión a cargo de:

Pacífico Editores S.A.C.
Jr. Castrovirreyna N.° 224-Breña
Central: 619-3720

Derechos Reservados conforme a la Ley de Derecho de Autor.
Este libro está expuesto a fe de erratas.
Queda terminantemente prohibida la reproducción total o parcial de esta obra por cualquier medio, ya sea informático, electrónico, mecánico, químico, óptico, incluyendo el sistema de fotocopiado, sin autorización escrita del autor e Instituto Pacífico S.A.C., quedando protegidos los derechos de propiedad intelectual y de autoría por la legislación peruana.

A Fiorella, el amor de mi vida

A mi familia, por su apoyo incondicional

A mis estudiantes, faros de luz

Y a Bianca 🐾*, por su cariño y lealtad*

AGRADECIMIENTOS

Esta obra no hubiese visto la luz sin el apoyo y las constantes palabras de aliento de Fiorella Chinchay, el amor de mi vida y una gran abogada. En estos dieciséis años, Fiorella me apoyó constantemente en todos y cada uno de mis proyectos académicos. Cuando el estrés y la ansiedad tocaban mi puerta, ella siempre estuvo tomando mi mano y dándome la tranquilidad y la fortaleza que necesitaba. Gracias a sus opiniones, mirada fresca pero siempre reflexiva, pude comprender el norte que debía guiar esta publicación. Escribir cada página demandó incontables amanecidas, por lo que aprendí a despertar antes que suene la alarma para velar de sus sueños como ella siempre ha cuidado de los míos.

Sería ingrato no incluir en estas palabras iniciales a mis padres, Ricardo y Juana Rosa, mis tías Isabel, Rosa y Victoria (†), y mi hermano Juan Diego, por inculcarme los valores y principios que han guiado mi formación profesional. Tengo la dicha de tener una maravillosa familia y compartir momentos de alegría que siempre atesoraré.

La ciberdelincuencia es un fenómeno de estudio reciente, por lo menos en el ámbito peruano; sin embargo, en este camino conocí a grandes profesionales -quienes han trazado un puente entre la Informática y el Derecho-, pero sobre todo magníficos seres humanos. A través de sus enseñanzas, pláticas e intercambio de opiniones, mi interés en el área fue incrementando. Gracias por sus valiosos aportes: Vladimir Padilla, Romy Chang, Miguel Morachimo, Óscar Montezuma, Fátima Toche, Víctor Espinoza Calderón, Wendy Requejo-Passoni, Marlon Luna, Juan Carlos Ortiz Pradillo, Daniela Dupuy, Marina Kiefer, Martín Nessi, Gustavo Pressman, Gustavo Sain, Martín Gershanik, Marcos Salt, Rafael García Borda, Agostina Miquelarena, Silvina Santangelo, Jorge L. Litvin, Sabrina Lamperti y Dévika Pérez.

A nivel institucional, expreso mi gratitud a la Pontificia Universidad Católica del Perú por brindarme la confianza y la oportunidad de ejercer la docencia universitaria y, de este modo, compartir reflexiones sobre la cibercriminalidad y la prueba digital. He tenido el privilegio de abordar estos temas en los cursos de pregrado *Comunicación Jurídica Eficaz*, *Derecho Procesal Penal Especial*, *Teoría de la Prueba* y *Clínica Jurídica: Derecho y Tecnología*, así como en el módulo especializado en delitos informáticos del curso *Nuevas Formas de Criminalidad*, en la Maestría en Derecho Penal.

Agradezco también a mis colegas, estudiantes y tesistas, con quienes he tenido el honor de trabajar en la investigación de esta área tan innovadora y llena de desafíos.

He de reconocer especialmente a quienes integran o han integrado tanto el Estudio Elías Puelles como el Observatorio Peruano de Cibercriminalidad, por su amistad y contribuir con mi crecimiento personal y desarrollo profesional: Rubén Vela, Andreina Camargo, Joseph Alguayo, Romina Alarcón, Flavia Martínez, Daniela Horna, Aldo Cabello, Bianca Reátegui, Fanny Herrera, Ariana Almeida, Valeria Dávalos, Yanira Obregón, Melissa Gonzáles y Rodrigo Villegas.

Finalmente, expreso mi más profundo reconocimiento a las empresas del sector tecnológico y a las víctimas que, a lo largo de estos años, han depositado su confianza en nuestro trabajo para ejercer su defensa frente al flagelo de la ciberdelincuencia. Su confianza nos ha permitido no solo afrontar con compromiso y determinación los retos que plantea este fenómeno en constante evolución, sino también contribuir al desarrollo de estrategias jurídicas más eficaces para la protección de sus derechos en el entorno digital.

A todos, muchas gracias.

PRÓLOGO

Es, sin duda, un privilegio y a la vez una responsabilidad prologar la obra de un autor cuya talla académica e intelectual impone respeto. Cuando el autor es, además, un referente nacional en su campo que goza de solvencia técnica, claridad expositiva y profundidad dogmática, y, a la vez, un colega de enorme proyección académica, cualquier palabra introductoria parece quedarse corta. No es tarea sencilla tratar de estar a la altura sin caer en lugares comunes ni en alabanzas vacías; se exige, en cambio, sensibilidad para captar el espíritu de la obra, y serenidad para reconocer —con humildad intelectual— que estamos ante un texto de referencia en el sector legal, tanto en el peruano como a nivel internacional.

Pero hay momentos en los que ese compromiso se transforma en una auténtica satisfacción personal. Así ocurre cuando la obra que se tiene entre manos ha sido escrita por alguien cuya trayectoria uno ha seguido con admiración desde sus inicios. Recuerdo con nitidez la primera vez que conocí a Ricardo Elías Puelles, hace ya más de una década, durante su paso por Toledo. Junto con juristas procedentes de nuestros hermanos países latinoamericanos, Ricardo se decidió a desafiar el frío invierno que azota las callejuelas y rincones de Toledo durante el mes de enero para cursar una maestría de Especialista en Garantías Constitucionales de la Investigación y la Prueba en el Proceso Penal que yo coordinaba en la Universidad de Castilla-La Mancha.

Aquel joven abogado peruano, de mente inquieta y mirada amable y educada, desbordaba una energía reflexiva que delataba vocación y profundidad inusuales para su edad. Había en él una mezcla singular de rigor técnico, curiosidad intelectual y sentido ético que me permitió intuir —con entusiasmo, casi con certeza— que estaba frente a alguien destinado a marcar huella. Gracias a él he tenido la suerte de visitar Perú y participar en labores formativas

y capacitadoras de diversos colectivos, a través del apoyo de la American Bar Association - Rule of Law Initiative (ABA ROLI Perú) y del Observatorio Peruano de Cibercriminalidad, que han impulsado excelentes programas de formación, así como investigaciones, publicaciones y propuestas normativas orientadas a fortalecer la respuesta del Estado frente a los delitos informáticos.

Ver hoy los frutos de aquella formación temprana, comprobar la proyección alcanzada por su trabajo académico, su influencia en la transformación legislativa de su país, y el respeto que cosecha dentro y fuera de las aulas, no solo ratifica lo que en su día fue una intuición, sino que brinda una satisfacción genuina, de esas que el oficio académico ofrece con cuentagotas: la alegría de haber acertado al confiar en el talento y la perseverancia de un joven jurista que, en efecto, ha llegado lejos... y que, todo indica, irá mucho más allá.

Pero, si Ricardo Elías Puelles atesora una enorme talla personal y académica, la obra que hoy tengo el gusto de prologar sobresale por méritos propios. La irrupción de las tecnologías de la información y la comunicación ha traído consigo beneficios extraordinarios en términos de desarrollo económico, acceso al conocimiento, innovación social y conectividad global. Sin embargo, este mismo entorno hiperconectado ha dado lugar a una nueva dimensión del crimen: la ciberdelincuencia, que no reconoce fronteras geográficas ni temporales, desafía las categorías jurídicas tradicionales y plantea retos sin precedentes en materia de investigación, persecución y cooperación internacional.

Nos encontramos ante una obra tan necesaria como rigurosa, que aborda el fenómeno de la ciberdelincuencia desde una óptica multifocal, jurídica y técnica, con un grado de precisión conceptual que pocas veces se alcanza en el tratamiento de esta compleja materia. El autor —jurista notable con sólida formación en tecnología de la información— ofrece un estudio profundo, meticuloso y sistemático de los principales delitos informáticos que afectan la integridad, disponibilidad y confidencialidad de los sistemas y datos, sin descuidar los marcos normativos que regulan su persecución y sanción.

El capítulo 1 sienta las bases del análisis con un abordaje panorámico de la ciberdelincuencia como fenómeno global. Se examinan las profundas transformaciones generadas por las tecnologías de la información y la comunicación en todos los ámbitos de la vida contemporánea: desde el ámbito económico, cultural y social hasta su lado más oscuro, como facilitadoras de nuevas formas

de criminalidad. El autor explora con sagacidad, y sobre todo con datos y evidencias contrastables, cómo esta realidad exige nuevos marcos normativos, capacidades institucionales especializadas y una mirada cada vez más transversal al delito. Sin duda, lo más sobresaliente de este primer capítulo introductorio se aprecia en la titánica labor autoral de clasificar las distintas modalidades comisivas. En el exhaustivo examen de los diferentes modos de ciberataques *puros*, el autor incluye también aquellos calificados como ciberataques *de contenido* (la distribución de contenidos ilícitos), así como los de evidente calado económico (fraude, espionaje o blanqueo de capitales) dentro de la concepción de ataques porque entiende que todos ellos atentan contra la seguridad informática.

El capítulo 2 realiza una revisión exhaustiva de los esfuerzos internacionales en la lucha contra la cibercriminalidad. Se analiza con maestría el rol pionero del Consejo de Europa, especialmente a través del Convenio de Budapest y sus protocolos adicionales, así como la legislación armonizada de la Unión Europea. También se examinan con detenimiento las resoluciones y estrategias impulsadas por la Asamblea General de las Naciones Unidas, sin dejar de lado el valioso aporte del Sistema Interamericano y las sucesivas reuniones de Ministros de Justicia y Procuradores Generales de las Américas desde 1999, que han consolidado mecanismos de cooperación regional frente a esta amenaza transnacional.

En el capítulo 3, el autor ofrece un valioso estudio comparativo y cronológico de la legislación penal peruana en la materia. Desde la tímida reforma de 1991 hasta la Ley N.º 30096 —piedra angular en la lucha contra los delitos informáticos en Perú—, se analiza la evolución normativa con especial énfasis en las reformas introducidas por la adhesión al Convenio de Budapest en 2019, así como las medidas más recientes plasmadas en el Decreto Legislativo N.º 1625 y la Ley N.º 32183, de 2024. Este apartado resulta clave para comprender cómo la legislación nacional ha ido asimilando estándares internacionales de cooperación, protección y persecución penal en el entorno digital.

Los capítulos siguientes abordan con profundidad las principales figuras típicas vinculadas a la delincuencia informática: el acceso ilícito, la interferencia en sistemas y datos, la interceptación de comunicaciones electrónicas, la utilización indebida de dispositivos, entre otros. Junto con un capítulo centrado en los aspectos generales de la normativa penal referida a la seguridad informática, los capítulos desde el quinto al noveno analizan cada uno de los tipos y sus

elementos. A partir de un sólido andamiaje teórico —con especial atención en el bien jurídico protegido, los elementos objetivos y subjetivos de los tipos penales, la concurrencia de delitos, agravantes y otras modulaciones típicas—, el autor nos guía a través de cada figura punible, desmenuzando con admirable claridad doctrinal y técnica los elementos que la configuran y distinguen.

La obra se culmina con un capítulo 10 que proyecta una mirada hacia el horizonte legislativo: los proyectos de ley sobre ciberdelitos contra la seguridad informática, que reflejan no solo una toma de conciencia del Estado frente al riesgo digital, sino también el esfuerzo constante por perfeccionar los instrumentos normativos que protejan a la ciudadanía y a las instituciones en el ciberespacio.

Este libro se justifica en la necesidad urgente de dotar a los operadores jurídicos —y a la sociedad en general— de herramientas conceptuales y dogmáticas sólidas que permitan comprender y combatir este fenómeno. No se trata únicamente de describir conductas punibles, sino de desentrañar su sustrato técnico, jurídico y social, identificando con precisión los bienes jurídicos afectados, las técnicas utilizadas por los delincuentes y las posibles respuestas del derecho penal.

La obra llena un vacío en la bibliografía especializada al ofrecer un análisis sistemático y comparado de los principales delitos informáticos, integrando no solo el enfoque normativo nacional (con especial atención a la evolución legislativa peruana), sino también el marco internacional en que estos ilícitos deben ser comprendidos y abordados.

Además, en un contexto donde la normativa evoluciona a gran velocidad y los proyectos de ley proliferan sin siempre contar con una base sólida, el rigor con el que el autor examina cada tipo penal resulta no solo oportuno, sino necesario. Al conjugar conocimiento técnico y jurídico, esta obra contribuye al desarrollo de una dogmática penal informática sólida, coherente y adaptable a los desafíos del siglo XXI.

Este libro no solo está destinado a juristas, fiscales, jueces y operadores del sistema penal. Es también una herramienta indispensable para los profesionales de las tecnologías de la información, legisladores, estudiantes e incluso usuarios que desean comprender los desafíos y respuestas que, como sociedad, debemos

articular frente a un fenómeno que —como bien muestra el autor— ha cruzado todas las fronteras.

No tengo duda de que este texto marcará un punto de referencia ineludible en el estudio de la criminalidad informática contemporánea. La claridad, el rigor y la profundidad con que se abordan las cuestiones más críticas del derecho penal y su interacción con la tecnología lo convierten en una obra imprescindible.

Ricardo Elías Puelles encarna el perfil del jurista contemporáneo: sólido en la teoría, comprometido con la práctica y profundamente consciente de los desafíos que plantea la criminalidad en entornos digitales. Su obra, su docencia y su liderazgo institucional lo convierten en una referencia ineludible para el estudio del derecho penal del siglo XXI. Y esta obra que hoy tengo el honor de prologar a buen seguro también contribuirá a elevar el nivel del debate público y técnico en esta materia y a fortalecer la respuesta del Estado frente a los delitos informáticos.

Madrid, en vísperas del solsticio de verano (23 de junio) de 2025

Juan Carlos Ortiz Pradillo
Universidad Complutense de Madrid

PRESENTACIÓN

La era informática, también llamada *era digital*, se inició en 1947 con la invención del transistor por parte de los científicos John Bardeen, Walter Brattain y William Shockley (premios nobel de física). A partir de ese año, la electrónica ha revolucionado la industria tecnológica al miniaturizar dispositivos que hoy en día han dado lugar a los teléfonos móviles, las computadoras portátiles y las *tablets* de última generación, así como muchos otros.

Hoy es posible que una persona que solo habla español pueda escuchar a otra que solo habla chino, en su propio idioma y únicamente utilizando unas gafas de sol tecnológicas; esto ha hecho que el idioma deje de ser una barrera para la comunicación entre las personas.

Y es que la evolución de las sociedades es un fenómeno imparable e inherente a la naturaleza del ser humano, el cual no solo se conforma con vivir, sino que aspira a hacerlo en cada vez mejores condiciones.

Es en este contexto en el que la obra *Delitos contra la seguridad informática*, del profesor Ricardo Elías Puelles, resulta fundamental para el estudio de los delitos y las nuevas formas de criminalidad que la revolución y la denominada era tecnológica traen consigo.

Así, por ejemplo, el tipo penal de hurto, que sanciona la típica sustracción de un bien mueble del lugar físico en el que se encuentra, hoy en día resulta insuficiente respecto de las sustracciones de dinero que se realizan ilícitamente de las cuentas en plataformas informáticas como Yape o Plin, o respecto de las clonaciones de tarjetas de crédito a partir de las cuales se retiran grandes sumas de dinero; y ni qué decir de las otras nuevas formas de comisión de delitos, como son los ciberataques puros, los ciberataques réplica o los ciberataques

de contenido, fenómenos de los que con mucha destreza y habilidad trata el profesor Elías Puelles a lo largo de su obra.

Este libro resulta fundamental para quienes desean acercarse a este mundo que genera una serie de nuevos delitos, pero, sobre todo, para quienes iniciamos la carrera de Derecho sin contar con un ordenador en nuestro hogar, y para quienes solíamos redactar nuestros trabajos recurriendo a la clásica, pero hoy ya sepultada, máquina de escribir.

La obra del profesor Ricardo Elías no solo estudia las normas de la materia, sino que también describe y analiza, con suma acuciosidad académica, cada uno de los aspectos que el legislador ha querido describir en cada una de las conductas tipificadas, destacando aquellos problemas donde se omite dar solución a los planteamientos trascendentales, los cuales, a criterio del autor, traen mayores riesgos interpretativos.

El profesor Elías, luego de una adecuada introducción donde nos hace reflexionar sobre lo "seguro" o "inseguro" de nuestra realidad, procede a analizar cada uno de los conceptos o denominaciones, términos nuevos o no tanto para algunos, pero necesarios para entender todo aquello que se quiere sancionar. Así, nos describe de manera adecuada qué debemos entender por *hacking, malware intrusivo, malware destructivo, ataques de insiders, ataques DoS 5, spam, ciberocupación, antisocial networks, ciberguerra o cyberwar, ciberactivismo o cyberhacktivism, ciberfraudes, phishing, pharming, scam, auction fraud, cyberspyware, uso de sniffers, ciberespionaje de empresas, identity theft; spoofing, DNS spoofing, ARP spoofing, IP spoofing, web spoofing, ciberblanqueo de capitales, ciberextorsión, ciberocupación, cyberstalking, cyberbullying, online harassment, sexting, extorsión con imágenes de sexting, online grooming, ciberespionaje terrorista, distribución de pornografía infantil en internet, ciberpiratería intelectual, online hate speech* y *ciberterrorismo.*

Podemos apreciar que son tan extensos y numerosos los nuevos conceptos que debemos aprender, ante lo cual resulta indispensable abrir nuestra mente a estas nuevas formas de comisión de delitos.

No obstante lo expuesto, la obra del profesor Elías no se queda en el mero estudio de las nuevas modalidades delictivas, sino que, en el capítulo 2, desarrolla con mucha destreza, todos los esfuerzos internacionales que han sido

realizados en la lucha contra la cibercriminalidad, tanto en el sistema europeo y en el sistema interamericano como en el sistema de las Naciones Unidas. Todo ello nos permite saber cuál es la situación en la que se encuentra el desarrollo normativo de estas nuevas figuras y, con ello, visualizar la urgencia de darle importancia a su adecuada tipificación y regulación normativa.

De igual manera, y como es muy propio de un académico completo como el profesor Ricardo Elías, este aterriza todos los temas descritos en su obra en el caso peruano, desarrollando en su capítulo 3 un estudio segmentado por periodos de la legislación peruana emitida en torno a los ciberdelitos contra la seguridad informática. Todo ello con la finalidad de, en los capítulos siguientes, realizar un análisis detallado sobre todos los aspectos establecidos en nuestra Ley de Delitos Informáticos.

Así, en las secciones que continúan, podremos apreciar diferentes formas de criminalidad, como el acceso ilícito o intrusismo informático, el atentado a la integridad de datos informáticos, el atentado a la integridad de sistemas informáticos, la interceptación ilícita de datos informáticos y el abuso de mecanismos y dispositivos informáticos; todas ellas temas que son de indispensable estudio y reflexión para quien desee especializarse en el ámbito penal.

Finalmente, en el capítulo 10, el profesor Ricardo Elías también aborda el estudio de los proyectos de ley relacionados a los ciberdelitos contra la seguridad informática que han sido presentados en el Perú, lo que completa la presente obra y permite al lector tener una visión del pasado, presente y futuro de este tipo de delitos en la legislación nacional.

Como resulta evidente, este libro constituye un gran e impecable esfuerzo, al recoger todo lo estudiado a nivel nacional e internacional sobre la materia en delitos cometidos por medios informáticos. No cabe duda de que la persistencia, dedicación y pasión que el profesor Ricardo Elías ha impreso en este estudio marcará un antes y un después en el desarrollo de estas figuras en nuestro país; todo lo que hace que este libro sea de obligatoria lectura para todos quienes nos vinculamos con los actuales medios tecnológicos.

Para nosotros es un honor que el profesor Ricardo Elías, gran penalista, gran procesalista penal, extraordinario amigo y magnífica persona, nos haya permitido participar en la elaboración del prólogo de este libro, el que es y

será siempre un fiel compañero para ilustrar todas las decisiones que requieran un conocimiento básico y profundo de los ciberdelitos contra la seguridad informática.

Lima, junio del 2025

Vladimir Padilla Alegre
Pontificia Universidad Católica del Perú

Romy Chang Kcomt
Pontificia Universidad Católica del Perú

ABREVIATURAS

0day	Zero Day o vulnerabilidad en software que no ha sido detectada
2FA	Two-factor Authentication o doble factor de autenticación
APT	Advanced Persistent Threat o amenaza persistente avanzada
ARP	Address Resolution Protocol o protocolo de resolución de direcciones
ATM	Automated Teller Machine o cajero automático
BEC	Business Email Compromise o Compromiso de correo empresarial
BTC	Bitcoin
CaaS	Crime as a Service o crimen como un servicio
CdPP	Código de Procedimientos Penales
CEO	Chief Executive Officer o director ejecutivo
CICTE	Comité Interamericano contra el Terrorismo
CISO	Chief Information Security Officer o director de seguridad de la información
CITEL	Comisión Interamericana de Telecomunicaciones
COMJIB	Conferencia de Ministros de Justicia de los Países Iberoamericanos
CP	Código Penal
CPP	Código Procesal Penal
CSIRT	Equipos de respuesta a incidentes de seguridad en computadoras

CVE	Common Vulnerabilities and Exposures o base de datos de vulnerabilidades conocidas
CVV	Card Verification Value o código de seguridad de tarjetas bancarias
DDoS	Distribuited Denial-of-Service o denegación de servicio distribuida
DNS	Domain Name System o sistema de dominio de nombres
DoS	Denial-of-Service o denegación de servicio
Doxx	Doxing
ENISA	European Union Agency for Cybersecurity o Agencia de la Unión Europea para la Ciberseguridad
FBI	Federal Bureau of Investigation o Buró Federal de Investigaciones de Estados Unidos
FTP	File Transfer Protocol
GB	Gigabyte
HTTP	Hyper Text Transfer Protocol
IA	Inteligencia Artificial
IDS	Intrusion Detection System o sistema de detección de intrusos
IMEI	International Mobile Equipment Identity o identidad internacional de equipo móvil
IMSI	International Mobile Subscriber Identity o identidad internacional del suscriptor móvil
IoT	Internet of Things o Internet de las cosas
IP	Internet Protocol
IPS	Intrusion Prevention System o sistema de prevención de intrusos
ISO	International Organization for Standardization u Organización Internacional de Normalización
LDI	Ley de Delitos Informáticos

MFA	Multi-Factor Authentication o autenticación multifactor
MITM	Man in the Middle o ataque de intermediario
NFT	Non-Fungible Tokens
NIST	National Institute of Standards and Technology o Instituto Nacional de Estándares y Tecnología de Estados Unidos
OPSEC	Operations Security o seguridad operativa
OSINT	Open Source Intelligence o inteligencia de fuentes abiertas
P2P	Peer to Peer
PL	Proyecto de ley
RAT	Remote Access Trojan o troyano de acceso remoto
REMJA	Reunión de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas
RN	Recurso de nulidad
RQ	Recurso de queja
SOCMINT	Social Media Intelligence o inteligencia en redes sociales
TB	Terabyte
TIC	Tecnología de la Información y Comunicación
TOR	The Onion Router o red anónima para navegación privada
TTPs	Tactics, Techniques, and Procedures
UE	Unión Europea
VPN	Virtual Private Network o red privada virtual

INTRODUCCIÓN

> Existe un concepto sobre el equilibrio que reza así: "Se puede ser 100 % seguro y 0 % funcional o 0 % seguro y 100 % funcional". Tu función consiste en ayudar a la organización a encontrar el equilibrio adecuado.
>
> *"No" no es una palabra estratégica*, Brian Gibbs[1].

I. ¿ESTAMOS SEGUROS EN EL CIBERESPACIO?

"Algún inescrupuloso ha creado un perfil falso en Facebook y está usando imágenes mías". "Alerta: Has realizado una compra con tu tarjeta de crédito, si no la reconoces, anúlala aquí: www.WebMaliciosa.com". "Su dispositivo celular ha sido ubicado a la(s) 06:47 pm. Ver localización en: www.TeRoboTusDatos.com". "Querido beneficiario: Nos comunicamos con usted respecto a sus fondos de compensación no reclamados de US$ 3.7 millones de dólares estadounidenses. Le informamos que se ha programado el pago de sus fondos a través de su banco, para lo cual debe responder este correo brindando la siguiente información: (1) Nombre completo, (2) País de origen, (3) Ciudad, (4) Dirección de casa, (5) Género, (6) Edad, (7) Ocupación, (8) Número de teléfono, (9) Código de país. Sírvase acompañar una copia de su documento de identidad y pasaporte actualizado".

Todos conocemos alguna víctima de suplantación de identidad, hemos recibido alguno de estos mensajes o, cuando menos, sabemos de alguien que lo ha hecho. En algunos casos, los correos van directamente al *spam* o simplemente los eliminamos porque dudamos de su veracidad. Sin embargo, algunas

1 Morillo, Christina (ed.). *97 cosas que todo profesional de la seguridad informática debería saber*. Madrid: Grupo Anaya, 2022, p. 37.

personas sí lo creen: brindan información sensible, acceden a páginas maliciosas y ese es tan solo el inicio de una vorágine de problemas. Lamentablemente, en muchos casos, las víctimas no tienen una orientación adecuada y se preguntan: ¿qué hago?, ¿a quién acudo?, ¿dónde denuncio?, ¿por qué le di clic al enlace?, ¿lo pude evitar?

Las víctimas de la cibercriminalidad no somos únicamente los ciudadanos, también lo son -y con mucha frecuencia- las empresas e, incluso, las instituciones gubernamentales. Un claro ejemplo sucedió, a fines del 2023, en Perú.

[Caso 1] El 11 de diciembre, la Secretaría de Gobierno y Transformación Digital publicó la Alerta Integrada de Seguridad Digital N.º 294-2023-CNSD[2]. En ella informó que, un día antes, el Equipo de Trabajo de Seguridad Digital de la Dirección Nacional de Inteligencia de la Policía Nacional del Perú detectó una publicación preocupante en la *dark web*: El grupo cibercriminal Lockbit 3.0 afirmaba que activos digitales de la policía peruana estaban comprometidos. Para demostrarlo, compartieron *screenshots* (capturas de pantalla) de la información que afirmaban tener en su poder.

Lockbit -de donde toma su nombre la organización criminal- es un *malware* (*software* malicioso) que encripta la información de la víctima y exige el pago de un rescate en criptomonedas a cambio de las llaves de descifrado. Si la víctima no paga, la información se hace pública. ¿Se imagina el lector si se diere a conocer información reservada como la identidad de agentes encubiertos, datos personales de testigos protegidos o informes de investigaciones reservadas?

El 22 de diciembre de 2023, la Dirección de Comunicación e Imagen Institucional de la Policía Nacional del Perú publicó el Comunicado N.º 21[3]. Precisaron que sus sistemas no fueron vulnerados:

2 Centro Nacional de Seguridad Digital. *Alerta integrada de seguridad digital N.º 294-2023. Lima: 11 de diciembre del 2023*. https://cdn.www.gob.pe/uploads/document/file/5550553/4934553-alerta-integrada-de-seguridad-digital-n-294-2023-cnsd.pdf

3 Fecha de última consulta: 14 de julio de 2024. Disponible en: https://www.policia.gob.pe/pnp/archivos/portal/doc/16276doc_COMUNICADO%20N%C2%B0%2021%20PNP.pdf

> En relación a una información difundida por redes sociales y medios de comunicación con respecto a la supuesta vulneración de los sistemas informáticos y base de datos de la Policía Nacional del Perú, por parte de *hackers* internacionales denominados Grupo Lockbit, se hace de conocimiento a la opinión pública:
>
> [...]
>
> 2. Actualmente, los sistemas informáticos policiales se encuentran funcionando en ambientes seguros, con total normalidad, bajo la supervisión constante de personal especializado, quienes efectúan la revisión de los archivos y la auditoría de los equipos de seguridad, a fin de identificar los orígenes de donde iniciaron la extracción de dichos datos de los centros de trabajo. Del mismo modo, es importante mencionar que los sistemas informáticos policiales no han sido vulnerados.

Llegado a este punto, el lector podría pensar: ¿La cibercriminalidad podría afectar nuestra salud o, incluso, poner en riesgo nuestras vidas? Lamentablemente debo responder con un ¡sí!, ya que cada ámbito o espacio está conectado a través de las TIC, por lo que no existe un ambiente totalmente seguro.

> **[Caso 2]** Así, por ejemplo, en setiembre del 2020, una mujer falleció durante un ataque de *ransomware* en un hospital de Dusseldorf, Alemania. Este ataque se dirigió contra los ordenadores de la Universidad de Dusseldorf, sin embargo, afectó los servidores de un hospital, encriptándolos. Toda vez que los sistemas no respondían, la paciente tuvo que ser trasladada de emergencia a otro nosocomio. Lamentablemente, falleció en el camino y es considerada la primera víctima mortal de un secuestro informático en el mundo[4].

Estos ejemplos demuestran cuán frágil puede ser la seguridad de nuestros sistemas informáticos y la necesidad de conocer estas nuevas modalidades. Así,

4 EUROPAPRESS. "Muere una mujer durante un ataque de 'ransomware' a un hospital de Dusseldorf (Alemania)". En: *Portaltic*, 18 de setiembre de 2020. https://www.europapress.es/portaltic/ciberseguridad/noticia-muere-mujer-ataque-ransomware-hospital-dusseldorf-alemania-20200918100804.html

frente al rápido e inminente avance de la criminalidad informática no solo es necesario tipificar adecuadamente estas nuevas conductas, sino también estudiarlas de manera detallada para buscar mecanismos de prevención y respuesta, como la Asociación Mundial de Derecho Penal reconoció en el XV Congreso Internacional de Derecho Penal realizado en 1994, esto es, hace más de treinta años:

> La comunidad académica y científica, conjuntamente con los gobiernos, deben comprometerse a realizar más investigaciones sobre el delito de la tecnología informática [...]. La teoría y política jurídica debe prestar especial atención al estudio y desarrollo de la ley informática, tomando en consideración las características específicas de la información, al compararla con los objetos tangibles, e investigar los probables cambios que afectan los principios generales y paradigmas[5].

Pese a que han transcurrido tres décadas, la labor pedagógica en esta materia es una tarea aún pendiente. El lector podrá comprobarlo fácilmente revisando la malla curricular de las universidades peruanas pues la ausencia de cursos específicos en cibercriminalidad o prueba digital es evidente. A nivel de posgrado, la oferta académica local también es escasa o, cuando menos, insuficiente. Hace 10 años, se promulgó la Ley N.º 30 096 o Ley de Delitos Informáticos. Esta norma marcó un hito en la lucha contra la cibercriminalidad -como se estudiará en el tercer capítulo de esta obra-, sin embargo, en este punto debo resaltar su quinta disposición complementaria final, pues en ella se subrayó la importancia del estudio y la capacitación de los operadores jurídicos en esta área:

> **Quinta.-** Las instituciones públicas involucradas en la prevención y represión de los delitos informáticos deben impartir cursos de capacitación destinados a mejorar la formación profesional de su personal -especialmente de la Policía Nacional del Perú, el Ministerio Público

5 Recomendaciones del XV Congreso Internacional de Derecho Penal. Sección II – Sobre delitos informáticos y otros delitos cometidos contra la tecnología informática. Evento realizado entre el 4 y 10 de septiembre de 1994, en Río de Janeiro - Brasil. Recomendación N.º 25. Asociación Mundial de Derecho Penal. "XV Congreso Internacional de derecho penal". En: *Anuario de Derecho Penal y Ciencias Penales* 1. Madrid: 1995, p. 381.

y el Poder Judicial- en el tratamiento de los delitos previstos en la presente Ley.

Ahora bien, al ser una especialidad del Derecho Penal relativamente nueva en nuestro país, de un lado, las investigaciones académicas locales son aún escasas y, de otro, contamos con pocas sentencias -y, muchos menos, pronunciamientos de la Corte Suprema de Justicia de la República-; es decir, tanto la doctrina como la jurisprudencia nacional aún son incipientes.

II. OBJETIVOS DE LA OBRA

Esta obra busca acercar al lector a la evolución de la ciberdelincuencia, tanto a nivel global como local. Desde el Derecho Penal, se analizan los delitos que atentan contra la seguridad informática: El acceso ilícito (art. 2 LDI), los ataques contra los datos y sistemas informáticos (arts. 3 y 4 LDI), la interceptación informática (art. 7 LDI) y el abuso de mecanismos y dispositivos informáticos (art. 10 LDI). En este sentido, no se aborda la ciberdelincuencia patrimonial -representada por el fraude informático o las estafas virtuales- ni la ciberdelincuencia que atenta contra la libertad e indemnidad sexual -cuyos casos más frecuentes son el *grooming* (proposiciones sexuales a niños, niñas y adolescentes por entornos virtuales) y la distribución de imágenes y videos de abuso sexual infantil (conocida erróneamente como pornografía infantil)-. Espero abordar estos fenómenos delictivos en próximas publicaciones.

Con la finalidad de facilitar la comprensión de algunas modalidades delictivas, en esta obra se emplea un lenguaje sencillo, evitando, de este modo, el uso de palabras o expresiones técnicas que, a veces, suelen generar confusión. No obstante, cuando, por necesidad, se emplean términos especializados, se utilizan ejemplos, gráficos o diagramas que permiten entender las ideas centrales que se buscan transmitir.

III. PRECISIONES TERMINOLÓGICAS

Actualmente, no existe consenso en la denominación que engloba el fenómeno delictivo aquí estudiado, pues recibe múltiples denominaciones: cibercrimen, ciberdelito, cibercriminalidad, ciberdelincuencia, criminalidad

informática, delito informático, etcétera[6]. Sin embargo, algunos especialistas los diferencian e identifican el tránsito del delito informático al cibercrimen[7]. Con fines metodológicos y tomando el debate conceptual planteado por Esteban Mestre Delgado, catedrático de Derecho Penal de la Universidad de Alcalá[8], a continuación, diferenciaremos estos términos:

iii.1. Delitos relacionados con los ordenadores

Es una traducción de la expresión anglosajona *computer-related crime*, manejada por el grupo de expertos convocado por la OCDE, en 1985, para el análisis y estudio de este nuevo fenómeno delictivo. A decir de Mestre Delgado, "se incluyen en esta configuración tanto las infracciones que se cometen utilizando medios o elementos informáticos o telemáticos, como aquellos cuya acción típica recae sobre los delitos informáticos"[9]. En el *Informe del Comité Europeo sobre problemas de delincuencia* se precisa que el objetivo fue buscar una definición amplia, pero funcional:

> Inicialmente se puede señalar que el comité, a lo largo de este estudio, utiliza el término "sistemasla informática" o "delito informático". En general, no se acepta ni reconoce ninguna definición para estos términos. El mencionado grupo de expertos que se reunió en el marco de la OCDE adoptó la siguiente definición como una definición de trabajo: "El abuso informático se considera como cualquier comportamiento ilegal, poco ético o no autorizado relacionado con el procesamiento automático y la transmisión de datos". El grupo de expertos no en-

6 Miró Llinares, Fernando. *El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio*. Madrid: Marcial Pons, 2012, p. 33.

7 Miró Llinares, *El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio*, cit., pp. 33-45; Gil Gil, Alicia y Roberto Hernández Berlinches (coords.), *Cibercriminalidad*. Madrid: Dykinson, 2019, pp. 154-156; Barrio Andrés, Moisés. *Delitos 2.0. Aspectos penales, procesales y de seguridad de los ciberdelitos*. Madrid: Wolters Kluwer, 2018, pp. 33-38.

8 Mestre Delgado, Esteban. "Introducción. Nuevas respuestas legales y jurisprudenciales frente a nuevas formas de criminalidad". En: Sanz Delgado, Enrique y Daniel Fernández Bermejo (coords.). *Tratado de delincuencia cibernética*. Navarra: Thomson Reuters / Aranzadi, 2021, pp. 48-51.

9 Mestre Delgado, "Introducción. Nuevas respuestas legales y jurisprudenciales frente a nuevas formas de criminalidad", cit., p. 48.

contró útil apuntar a una definición más precisa, sino que eligió una clasificación funcional[10] [Traducción propia].

iii.2. Delitos informáticos

Es una traducción de la también expresión anglosajona *computer crime*. En *The OECD Observer*, de 1986, se recoge una reflexión que sintetiza la inicial confusión terminológica, ya que, hacia 1982, conceptualizar la expresión *delitos informáticos* era una labor muy compleja:

> Cuando comenzaron las discusiones sobre tales asuntos en la OCDE en 1982, nadie sabía realmente qué constituía el delito informático en términos legales. La tarea de definirlo y enmarcar la legislación adecuada es lo que un grupo de expertos está tratando de hacer ahora. El informe del grupo establece las cuestiones, indicando en detalle su complejidad técnica, política, legal y ética inherente[11] [Traducción propia].

En 1989, Donn B. Parker publicó *Computer Crime: Criminal Justice Resource Manual* [*Delitos informáticos: Manual de Recursos en Justicia Penal*] para el Departamento de Justicia de los Estados Unidos de América. En dicha obra, utiliza la expresión *delitos informáticos*, pero le confirió un significado mucho más amplio al previamente estudiado:

> Los delitos relacionados con las computadoras -una categoría amplia- son cualquier violación de las leyes penales que impliquen conocimiento de la informática para su perpetración, investigación o enjuiciamiento. Pese a que los delitos relacionados con las computadoras son principalmente delitos de cuello blanco, cualquier tipo de acto ilegal basado en la comprensión de la informática puede ser un delito relacionado con las computadoras. Incluso, podrían ser delitos violentos que destruyen computadoras o su contenido y, en consecuencia, pone en riesgo la vida humana (por ejemplo, de personas que depen-

10 Council of Europe. *Computer-related crime. Recommendation N.º R (89) 9 on computer-related crime and final report of the European Committee on Crime Problems.* Strasbourg, 1990, p. 13.

11 Organisation for Economic Co-Operation and Development. "Computer crime". En: *The OECD Observer* 142, septiembre. Paris: 1986, p. 20

> den del correcto funcionamiento de las computadoras para su salud o bienestar). La proliferación y el uso de computadoras personales hacen que los delitos relacionados con las computadoras sean potencialmente endémicos para toda la sociedad.
>
> [...] A los efectos de este manual, el término más simple de delito informático ha sido usado para referirse generalmente a tres categorías: delitos informáticos en sentido estricto, delitos relacionados con la informática y abuso informático[12] [Traducción propia].

Mestre Delgado advierte que existen diversas posiciones conceptuales en torno a este término. Según cierto sector, entre los que sitúa a Romeo Casabona, se circunscribe a los casos en los que destaca la tecnología sobre o a través de la que actúa esa delincuencia. De este modo, hay quienes restringen esta clasificación solo a los delitos que afectan a los datos o a la información contenida en los sistemas informáticos. En sentido contrario, Mata y Martín afirma que "habría que incluir exclusivamente los supuestos en los que el ordenador representa el medio de ejecución, pues sólo en éstos se aprecian las peculiaridades y características de los sistemas informáticos o del procesamiento electrónico de datos que convierten estos hechos en algo novedoso, diverso, al menos desde un punto de vista criminológico"[13]. En este punto, el lector debe recordar la denominación de nuestro ordenamiento especial: Ley N.° 30096 o Ley de Delitos Informáticos.

La expresión lingüística *delito informático*[14] empezó a ser utilizada en la década de los setenta para referirse a los ilícitos relacionados con la informática[15],

---

12 Parker, Donn B. *Computer Crime: Criminal Justice Resource Manual*. Washington D. C.: National Institute of Justice, 1989, p. 2. La primera edición la publicó en 1979, en coautoría con Susan Nycum: *Criminal Justice Resource Manual on Computer Crime* (SRI International).

13 Citado por Mestre Delgado, "Introducción. Nuevas respuestas legales y jurisprudenciales frente a nuevas formas de criminalidad", cit., p. 49.

14 Recomiendo el capítulo ¿Existe la categoría "Delitos Informáticos"? para comprender su uso y difusión. En: Riquert, Marcelo A. *Delincuencia informática en Argentina y el Mercosur*. Buenos Aires: Ediar, 2009, pp. 31-38.

15 Algunos autores identifican los delitos informáticos con los *computer crimes*: Gil Gil/ Hernández Berlinches, *Cibercriminalidad*, cit., p. 154; Barrio Andrés, *Delitos 2.0. Aspectos penales, procesales y de seguridad de los ciberdelitos*, cit., p. 33. En la misma línea: "Cuando se habla de este tipo de criminalidad, el significado más utilizado en

pues esta se erigía como el medio u objeto para su comisión. Algunos países, como el Perú, continúan utilizando este término.

iii.3. Criminalidad informática

Es una traducción de la expresión alemana *Computerkriminalität,* la cual resalta el carácter criminológico del fenómeno estudiado. Según Juan Carlos Menéndez y María Eugenia Gayo, los delitos informáticos se refieren únicamente a las conductas ilícitas tipificadas en el ordenamiento penal; en cambio, la delincuencia o criminalidad informática "al ser más genérica, permite englobar las diferentes modalidades delictivas vinculadas con las nuevas tecnologías"[16].

iii.4. Delitos tecnológicos

Para el magistrado español Eloy Velasco Núñez, junto al concepto instrumental de los delitos informáticos, encontramos el de delitos tecnológicos, el cual trata de "agrupar aquellos delitos que, en parte o en todo, se desarrollan a través de las nuevas tecnologías, y que, además de internet y la informática, pretenden agrupar bajo su denominación los que se producen a través o contra otras nuevas tecnologías como el *cloud computing*, el tratamiento del *big data*, el internet de las cosas, el *blockchain*, la inteligencia artificial"[17].

iii.5. Ciberdelincuencia o cibercriminalidad

El uso del término ciberdelito o cibercrimen ha proliferado desde la década de los noventa y es la traducción del anglicismo *cybercrime*[18], el cual está

términos prácticos es aquel que los describe como conductas indebidas e ilegales donde interviene un dispositivo informático como medio para cometer un delito o como fin u objeto del mismo" (Sain, Gustavo y Horacio Azzolin. *Delitos informáticos. Investigación criminal, marco legal y peritaje.* Buenos Aires: B de F, 2018, p. 8).

16 Menéndez Mato, Juan Carlos y María Eugenia Gayo Santa Cecilia. *Derecho e informática. Ética y legislación.* Barcelona: Bosch, 2014, p. 319.

17 Velasco Núñez, Eloy. *Delitos tecnológicos. Cuestiones penales y procesales.* Madrid: Wolters Kluwer, 2021, p. 23. Es importante precisar que este autor diferencia los delitos informáticos en sentido estricto y en sentido lato. En el primer grupo se encuentran los ilícitos cometidos *contra* la informática; en el segundo, los cometidos *a través* de la informática.

18 La Dra Marcum, profesora de la Appalachian State University, define el cibercrimen en los siguientes términos: "The destruction, theft, or unauthorized or ilegal use, mo-

compuesto por el prefijo *cyber*, que proviene del término *cyberspace* -término acuñado por el escritor de ciencia ficción William Gibson-. A diferencia de los delitos informáticos, este concepto se erige alrededor del Internet y de las TIC. Así, una concepción amplia del cibercrimen lo define adecuadamente como "aquel delito cuya característica esencial es el rol central que las TIC juegan en su comisión"[19]. Para Mestre Delgado, "son expresiones más evolucionadas y vinculadas con el desarrollo e implementación mundial de Internet y las redes de transmisión de datos, que priorizan este último aspecto en detrimento de la mera existencia de un sistema informático[20]". De ahí que Moisés Barrio sostenga que nos encontramos frente a delitos 2.0 que "están absolutamente determinados por el uso de Internet y de las TIC"[21] y que comprenden tanto (i) los delitos específicos de Internet, (ii) los delitos asistidos electrónicamente como (iii) aquellos cuya comisión implica un aspecto electrónico significativo.

A nivel legislativo, uno de los principales instrumentos internacionales al que nos hemos adherido utiliza una expresión afín. Me refiero al Convenio de Budapest o Convenio sobre la Ciberdelincuencia. De la misma forma, a fines del 2024, la Asamblea General aprobó la Convención de las Naciones Unidas contra la Ciberdelincuencia.

En Perú, como se ha dicho anteriormente, en octubre de 2013, se publicó la Ley de Delitos Informáticos. Si bien el nombre de este cuerpo legislativo incluye la expresión *delito informático*, su primer artículo emplea el término *ciberdelincuencia* para delimitar el objeto de protección:

> **Art. 1 LDI.-** La presente Ley tiene por objeto prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización

---

dification, or copying of information, programs, services, equipment, or communication networks" (Marcum, Catherine D. *Cyber crime.* 2.ª edición. New York: Wolters Kluwer, 2019, p. 3).

19 Miró Llinares, *El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio,* cit., p. 43.

20 Mestre Delgado, "Introducción. Nuevas respuestas legales y jurisprudenciales frente a nuevas formas de criminalidad", cit., p. 50.

21 Barrio Andrés, *Delitos 2.0. Aspectos penales, procesales y de seguridad de los ciberdelitos*, cit., p. 36

> de tecnologías de la información o de la comunicación, con la finalidad de garantizar la **lucha eficaz contra la ciberdelincuencia** [El resaltado es mío].

IV. ESTRUCTURA DE LA OBRA

Esta obra está dividida en diez capítulos:

En el primer capítulo, titulado "La ciberdelincuencia, un fenómeno global", se analiza el impacto de las TIC en el desarrollo económico y en la comisión de delitos -tanto en la facilitación de ilícitos tradicionales como en la configuración de nuevas formas de criminalidad-. Además, se explica el tránsito temporal de los delitos informáticos a los ciberdelitos, desarrollando, a su vez, tres tipos de ataques: puros, réplica y de contenido. Con la finalidad de diferenciarlos, se proponen definiciones y se presentan ejemplos de cada uno de ellos.

El segundo capítulo recoge una reseña de los principales esfuerzos internacionales en la lucha contra la ciberdelincuencia, resaltando el Convenio de Budapest al habernos adherido en el 2019 y la Convención de las Naciones Unidas contra la Ciberdelincuencia, aprobada por la Asamblea General en diciembre del 2024.

En el tercer capítulo, transitamos por los hitos más importantes de la legislación penal peruana en lo que a la lucha contra los ciberdelitos se refiere. Así, se analiza el Código Penal originalmente publicado y luego se explican los motivos de sus posteriores modificaciones, las cuales llegaron a su momento cumbre en el 2000, año en el que son incorporados los delitos informáticos.

En el cuarto capítulo, titulado "Aspectos generales", se aborda la función preventiva y retributiva de la LDI, se desarrolla conceptualmente la diferencia entre sistemas y datos informáticos, así como los elementos que integran la seguridad informática. Además, se fundamentan las razones por las que el bien jurídico protegido es, precisamente, la seguridad informática y no otros bienes tradicionales como la intimidad o la propiedad. Finalmente, se reflexiona sobre la errónea técnica legislativa que trajo la modificación de la LDI en marzo del 2014: incluir (innecesariamente) los elementos *deliberada* e *ilegítimamente* (artículo 2) en la legislación bajo estudio.

Desde el quinto hasta el noveno capítulo de esta obra, se intenta contribuir al debate académico nacional, analizando el delito de acceso ilícito o *hacking* (cap. quinto), el delito de ataque a los datos informáticos (cap. sexto), el delito de ataque a los sistemas informáticos (cap. séptimo), el delito de interceptación ilícita de datos (cap. octavo) y el delito de abuso de mecanismos y dispositivos informáticos (cap. noveno). Para ello, empleo el siguiente esquema de análisis:

En primer lugar, concuerdo cada norma con el Convenio sobre la Ciberdelincuencia o Convenio de Budapest, vigente en Perú desde el 01 de diciembre del 2019[22]. Además, el lector encontrará el desarrollo específico que se efectúa en el Informe Explicativo del referido Convenio. De esta forma, cada artículo podrá ser confrontado con el instrumento de carácter normativo que ha sido ratificado por más de 60 países en el mundo. Aunado a ello, se contrasta con la regulación propuesta en la Convención de las Naciones Unidas contra la Ciberdelincuencia, de reciente aprobación.

En segundo lugar, cada delito es analizado desde la legislación comparada iberoamericana -tomando como marco de referencia a los países que se han adherido al Convenio de Budapest[23]-. La finalidad de este apartado es comprender las similitudes y diferencias que existen en nuestros países, resaltando que somos el único en el que se agregó -insisto, innecesariamente- las expresiones *deliberada* e *ilegítimamente*.

En tercer lugar, se desarrolla la génesis legislativa de cada ilícito estudiado, su regulación actual y se propone una definición que permita comprender los alcances de cada verbo rector para evitar incoherencias al realizar el respectivo juicio de subsunción. Adicionalmente, se incluyen ejemplos que permiten -espero- comprender las diferentes y potenciales modalidades delictivas. Finalmente, a partir del estudio y reflexión, se presentan propuestas normativas de *lege ferenda*.

22 Poder Ejecutivo. *Decreto Supremo N.º 010-2019-RE, Ratifican el Convenio sobre la Ciberdelincuencia*. Lima: 10 de marzo de 2019.

23 Fariña, Cristian; Alexis Blasco y Fernando Dedovich. "Legislación comparativa sobre cibercrimen en Latinoamérica". En: Dupuy, Daniela (dir.) y Mariana Kiefer (coord.). *Cibercrimen. Aspectos de derecho penal y procesal penal. Cooperación internacional. Recolección de evidencia digital. Responsabilidad de los proveedores de servicios de Internet*. Montevideo: B de F, 2019.

En el décimo y último capítulo, el lector encontrará cada uno de los proyectos que originaron la promulgación de la LDI, así como su posterior modificación. Se incluye la redacción de la propuesta original, así como cada exposición de motivos por la riqueza de su contenido: casos que acontecieron en la realidad nacional, cifras y estadísticas que preocuparon al legislador, motivaciones políticas que trajeron la redacción y el cambio, entre otros. Considero que cada proyecto de ley debe ser estudiado para comprender íntegramente nuestra legislación actual. Además, se incluyen comentarios a cada proyecto de ley resaltando su trascendencia y posibles áreas de oportunidad que deberían ser aprovechadas en futuros debates legislativos.

Esta obra incluye una sección de anexos, la cual comprende tres secciones:

A. Línea de tiempo de los principales eventos o instrumentos

B. Dictamen de la Comisión de Justicia y Derechos Humanos recaído en los proyectos de ley 034/2011-CR, 307/2011-CR y 1136/2011-CR, 26 de junio de 2012

C. Diario de Debates, 12 de setiembre de 2013

Estos anexos buscan que el lector profundice sobre las razones y discusiones que giraron en torno a los ciberdelitos contra la seguridad informática. Quizás, en algún momento, respalden eventuales reformas legislativas o sean empleados como fuente de investigación para estudios especializados en la materia.

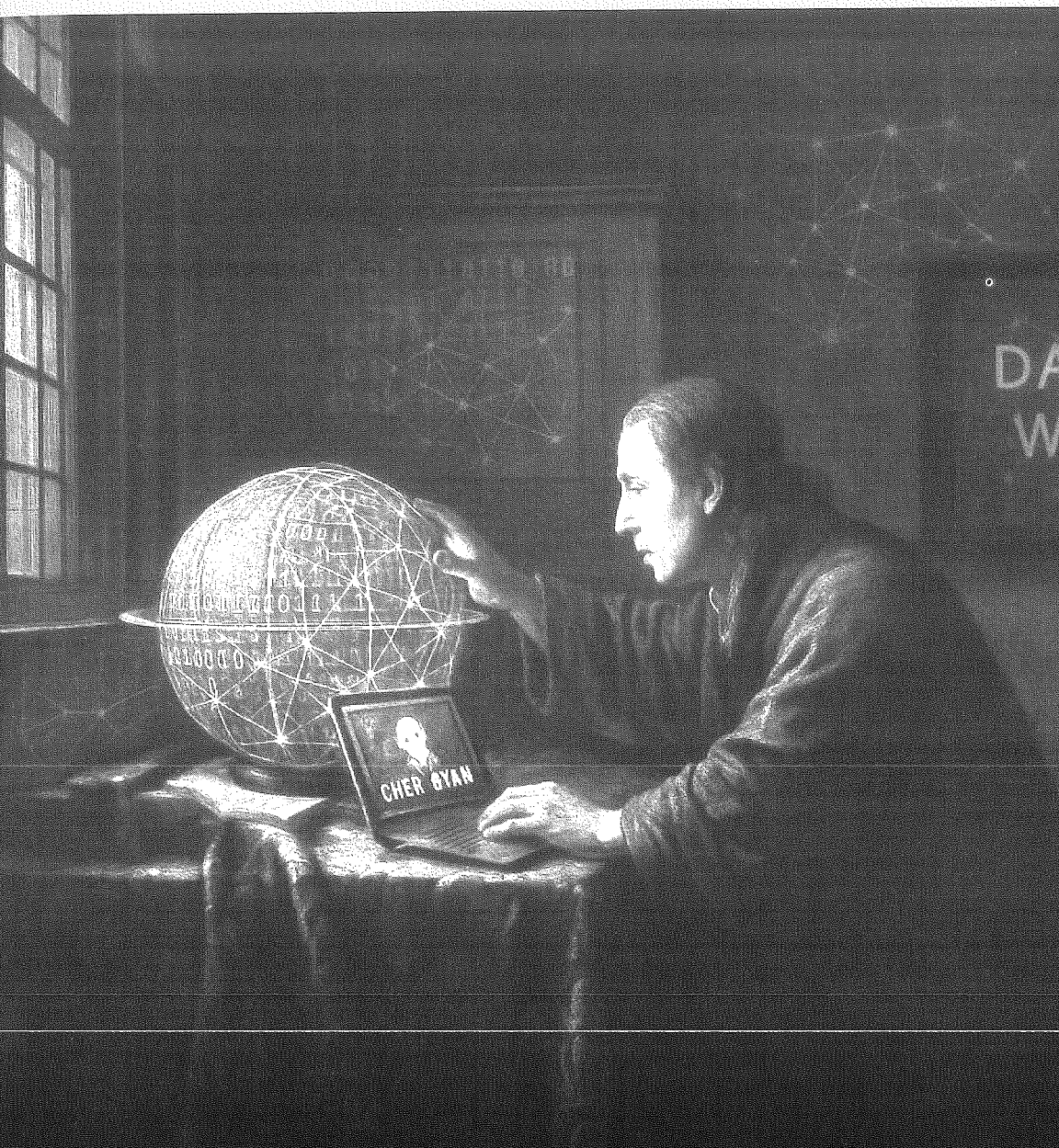
Esta obra recoge reflexiones personales que se han nutrido de fructíferas charlas con grandes maestros y amigos, así como del intercambio de ideas e inquietudes que naturalmente nacen en las aulas universitarias y en las capacitaciones a las que inmerecidamente he sido invitado a participar. Espero, con mucha ilusión, que el lector encuentre en estas páginas un insumo útil para el quehacer jurídico.

Lima, abril de 2025

Ricardo N. Elías Puelles

CAPÍTULO 1

LA CIBERDELINCUENCIA COMO UN FENÓMENO GLOBAL



* La ilustración de la página anterior corresponde a una adaptación de *El astrónomo*, de Johannes Vermeer (1669). Para su elaboración, se empleó una de las herramientas de generación de imágenes de la empresa OpenAI.

CAPÍTULO 1

LA CIBERDELINCUENCIA COMO UN FENÓMENO GLOBAL

Sumario: 1.1. Introducción. 1.2. De internet a la sociedad de la información. 1.3. El impacto global de las tecnologías de la información y comunicación. 1.4. Ciberataques puros, réplica y de contenido. 1.5. Conclusiones del capítulo.

¿Hemos advertido que la palabra *documento* no significa mucho hoy en día? Lo cubre todo, desde un archivo de texto de un procesador de textos a una hoja de cálculo para una aplicación Java incluida en una página web interactiva.

No solía ser así. Un documento era un pedazo de papel -como un testamento o un pasaporte- con un rol oficial en nuestro ordenamiento jurídico. Pero cuando los fabricantes de procesadores de textos se plantearon cómo denominar a su tipo especial de archivos, importaron el término *documento*. A medida que los archivos de texto incorporaron elementos multimedia, la palabra se ensanchó hasta el punto de carecer de sentido. Para tratar de distinguir los tipos de archivo, Windows 95 puso en su menú la extensión Documento.

El hecho de que ni siquiera podamos decir lo que es un documento ya indica la profundidad del cambio que estamos experimentando en la forma en que interactuamos con la información y, en última instancia, con nuestro mundo.

David, WEINBERG. *What´s a Document*[24]

24 Citado por PONS, Anaclet. *El desorden digital. Guía para historiadores y humanistas.* Madrid: Siglo XXI, 2013, p. 180.

1.1. INTRODUCCIÓN

Son las 06:00 am, suena la alarma desde un celular, mientras vibra el *smartwatch* que controla el sueño de Fiorella. Se levanta, enciende su *smart* TV, accede a su cuenta de YouTube para ver el resumen de noticias, pues el cable quedó en el olvido. Desbloquea su celular, revisa sus mensajes en WhatsApp y en Telegram, comparte algunos comentarios por X (Twitter), abre Spotify y le pide a Livi -la DJ generada por IA- que seleccione algunas canciones para iniciar el día. Mientras sale de la ducha y esquiva a su aspiradora robot -que conoce cada centímetro del departamento-, recibe un mensaje: "Se realizó el cobro mensual de tu membresía en LinkedIn". Se dirige a una reunión fuera de su oficina y, como no conoce la dirección, la escribe en Waze. Estaciona en Starbucks por su café y paga con puntos desde la aplicación -no sin antes actualizarla-. Sube una foto del local a sus historias de Instagram antes de llegar a su destino. Como será un encuentro breve, utiliza Goodnotes en su iPad para tomar algunos apuntes. La sesión finaliza, pero sus notas ya están sincronizadas en todos sus dispositivos.

El impacto de la tecnología en el quehacer diario es tan profundo y habitual que, a veces, olvidamos cómo ha transformado nuestras actividades, nuestras vidas. Al igual que los múltiples beneficios que genera, también abre un abanico de nuevos delitos o facilita otros tantos con los que ya convivíamos.

El objetivo de este capítulo es conocer el impacto global de las TIC, así como el "novedoso" fenómeno delictivo denominado *cibercriminalidad*. A través del estudio de casos especialmente seleccionados, se analizará la basta tipología existente -que ha sido graficada por el catedrático español Fernando Miró Llinares como el *Bestiario del ciberespacio*[25]-.

1.2. DE INTERNET A LA SOCIEDAD DE LA INFORMACIÓN

El origen de Internet se sitúa en el contexto de la Guerra Fría, remontándose específicamente a 1968, y está asociado a ARPANET[26], la primera

25 Miró Llinares, *El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio*, cit., p. 229.

26 El acrónimo ARPANET proviene de Advanced Research Projects Agency Network o Agencia de Proyectos de Investigación Avanzados.

red experimental construida por el Network Information Center (NIC), que conectó su computadora con la de la Universidad de California (UCLA) en Los Ángeles. Poco tiempo después, el 29 de octubre de 1969, dos programadores lograron enviar el primer mensaje entre la UCLA y el Instituto de Investigación de Stanford, convirtiéndose así en los primeros nodos de ARPANET[27].

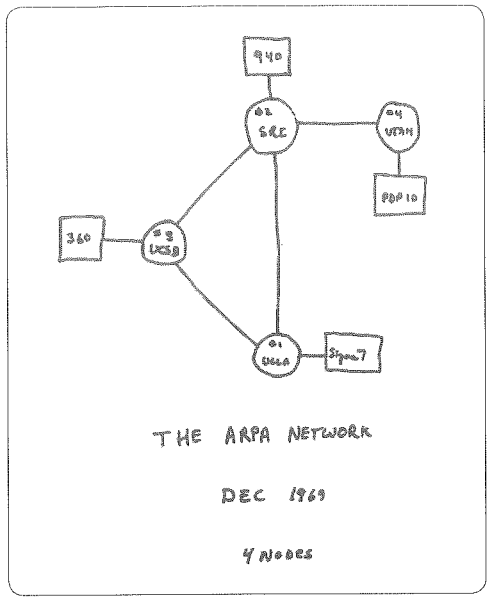


Imagen 1: El inicio de Internet. Un boceto de la red ARPA de 1969[28].

Este proyecto se originó como un programa militar diseñado para mantener disponibles y operativas las computadoras manejadas por la milicia, contratistas de defensa y universidades, en caso algún canal o punto de comunicación fuese atacado o dañado. De manera paralela, se desarrolló el MILNET, una red militar con la que se intercambiaba información.

27 Schjolberg, Stein. *The history of cybercrime.* 3.ª edición. Cybercrime Research Institute, 2020, p. 15.

28 Imagen tomada de: Kenyon, Henry. "The network of our times. A DARPA perspective on the development of the internet". En: *DARPA. Defense Advanced Research Projects Agency, 1958-2018.* Tampa (FL.): Faircount Media Group, 2018, p. 103. https://www.darpa.mil/sites/default/files/attachment/2025-02/magazine-darpa-60th-anniversary.pdf

En octubre de 1972, Robert Khan, quien se ocupó del diseño de la arquitectura global de ARPANET, organizó y demostró, por primera vez, su funcionamiento en la International Computer Communication Conference. Ese mismo año, Ray Tomlinson envió el primer *mail* y propuso la utilización del símbolo arroba @ como elemento que permitiría distinguir una dirección de correo electrónico. En esta época, ya se contabilizaban 23 equipos conectados a ARPANET[29], número que aumentó rápidamente dada su importancia y utilidad:

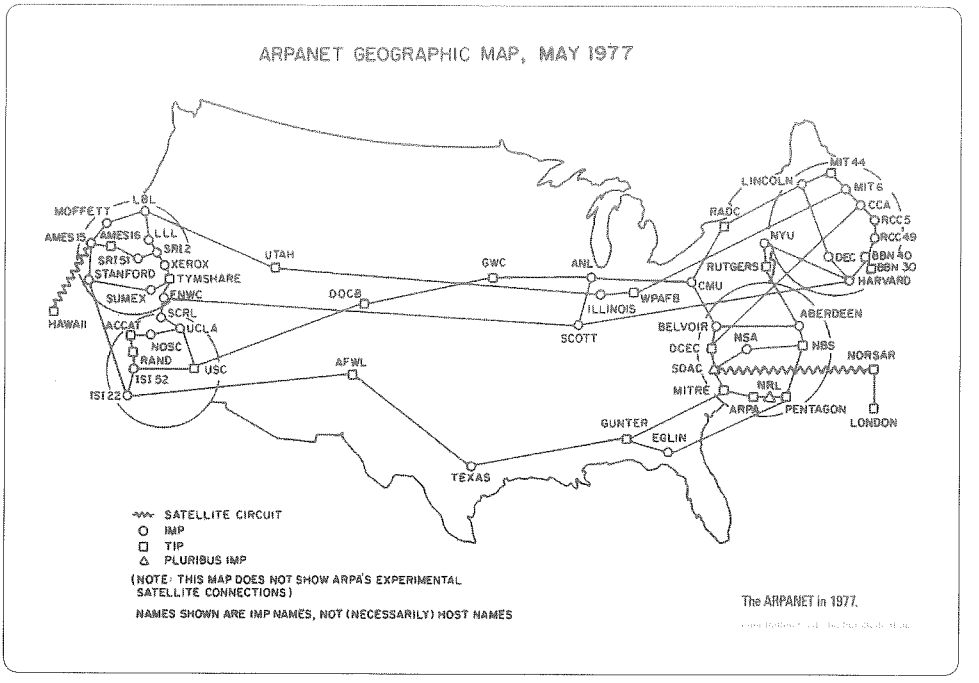


Imagen 2. ARPANET, 1977[30].

Durante esta década, se inventó el primer sistema de comunicaciones común: NCP o Network Control Protocol -que sería reemplazado en 1983 por el vigente TCP/IP-. De hecho, la interconexión mediante TCP/IP entre

29 Barrio Andrés, Moisés. *Fundamentos del derecho de internet*. 2.ª edición. Madrid: Centro de Estudios Políticos y Constitucionales, 2020, p. 83.

30 Imagen tomada de: Kenyon, "The network of our times. A DARPA perspective on the development of the internet", cit., p. 104.

ARPANET, MILNET y CSNET[31] es considerado como el momento histórico del nacimiento de Internet. Entre otros proyectos afines, es importante destacar también la creación del terminal virtual o *telnet*, la transferencia de ficheros (FTP), el sistema de nombres de dominio (DNS), los grupos de discusión (*news*), la Web (WWW) y el *chat* en tiempo real[32]. En esta época se acuña y difunde el uso del término *ciberespacio* como sinónimo de *internet*[33].

En 1986, nació la National Science Foundation (NSF) para facilitar el acceso a su centro de supercomputación. Con el objetivo de evitar los trámites burocráticos requeridos para conectarse a ARPANET, la NSF creó su propia red: la NSFNET. Esto originó el aumento de conexiones y el establecimiento de otras redes interconectadas que, poco a poco, se consolidó y originó que, en 1990, ARPANET dejara de funcionar.

La década de los noventa generó el uso masivo y comercial de Internet, como hoy en día lo conocemos. El profesor Barrio Andrés resume algunos eventos importantes en los siguientes términos:

> Así, en 1991, la NSF levantó la prohibición comercial, permitiendo la emergencia de los mercados virtuales 24/7 que conocemos hoy. Los primeros anuncios publicitarios aparecieron en 1994 para Zima, una bebida alcohólica. Ese mismo año, la Casa Blanca lanzó su sitio web, y la palabra *spam* se convirtió en parte del léxico popular. En 1994, relativamente pocas empresas, bufetes de abogados y asociaciones profesionales disponían de una página web. Ese mismo año, una gran compañía, Pizza Hut, empezó a aceptar pedidos en línea. En 1994, un

31 El acrónimo CSNET proviene de Computer Science Network o Red de Ciencias Computacionales.

32 Barrio Andrés, *Fundamentos del derecho de internet*, cit., p. 87

33 "El término ciberespacio fue adoptado tras la publicación de una obra de ciencia ficción de 1982 del autor William Gibson denominada "Burning Chrome" y popularizada a través de otra de sus obras del año 1984 titulada "Neuromancer". Durante la década de los 90s el término se empezó a utilizar como un sinónimo de facto para internet, y subsecuentemente para referirse a la World Wide Web (WWW), particularmente en los círculos académicos donde se originó el protocolo IP que posteriormente daría lugar a la creación y difusión de internet a nivel comercial" (Velasco San Martín, Cristos y Andrés Velázquez. *Aspectos prácticos de los ciberdelitos y la evidencia digital*. Valencia: Tirant lo Blanch, 2021, p. 36).

> *hacker* anónimo lanzó el "Good Time Virus", que se reputa como uno de los primeros virus del ciberespacio.
>
> También ese mismo año, America Online se conectó a internet por primera vez. En 1994, Amazon.com, la librería más grande del mundo, fue fundada, y Yahoo! fue lanzado. Al año siguiente, Microsoft presentó su sistema operativo Windows 95 el 25 de agosto de 1995, que incorporaba de serie el navegador Internet Explorer y el protocolo TCP/IP (cosa que no hizo ni MS-DOS ni Windows 3.1). Los primeros casinos de juego por Internet se organizaron en 1995. En setiembre de 1995 se liberalizó algo el registro de nombres de dominio. También en ese año hicieron aparición otros navegadores web, como fue el caso de Mosaic, que contribuyeron a hacer más popular la navegación por Internet[34].

El siglo XXI comenzó con la crisis de las empresas "punto com", muchas de las cuales fueron valoradas en miles de millones de dólares sin ser realmente rentables. Esto provocó una recesión en Estados Unidos en octubre de 2002, con impacto a nivel global. A pesar de ello, la evolución de Internet continuó, dando lugar a nuevas formas de comunicación, como la distribución de contenido a través de redes P2P, el *streaming* en redes sociales y *microblogging*, el desarrollo del Internet de las Cosas (IoT), la tecnología *blockchain*, entre otras innovaciones de la Web 2.0[35].

Dada la (r)evolución tecnológica, actualmente se utiliza la expresión *Sociedad de la Información* para "referirnos al uso de las tecnologías de la información y la comunicación como el medio a través del cual se tiene acceso a diversas fuentes de información que enriquecen la cultura y el conocimiento

34 Barrio Andrés, *Fundamentos del derecho de internet*, cit., pp. 93 y s.

35 "[El] término web 2.0 ha alcanzado bastante popularidad para hacer referencia a las características de ciertos servicios y plataformas que han coadyuvado a la rápida transformación experimentada por el modo en el que los internautas interactúan en la Red, siendo sus exponentes más representativos los *blogs*, las redes sociales y los *wikis*, así como en general las redes que permiten compartir y difundir contenidos generados por los propios usuarios (UCG, *User-Generated Content*). También se incluyen en esta categoría los entornos que permiten compartir recursos de todo tipo -así, documentos (Google Drive y Office 365), videos (YouTube, Vimeo, Dailymotion, Dalealpay...), fotografías (Instagram, Picasa o Flickr), agregadores de noticias (Digg, Reddit, Menéame), almacenamiento en la nube (Dropbox, Google Drive, One Drive), etc.-". Ibid. pp. 97 y s.

del ser humano"[36]. En las líneas siguientes, precisamente, abordaré el impacto positivo y negativo de las TIC y su relación con la cibercriminalidad.

1.3. EL IMPACTO GLOBAL DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

1.3.1. Las tecnologías de la información y la comunicación

En octubre del 2013, se publicó la Ley N.° 30096 o Ley de Delitos Informáticos. El objeto de esta norma es prevenir y sancionar las conductas ilícitas "cometidas mediante la utilización de tecnologías de información o de la comunicación" (art. 1 LDI). Toda vez que este artículo precisa el medio comisivo de los ciberdelitos, será importante conceptualizarlo y entender sus limitaciones. En este sentido, el acrónimo TIC hace referencia a las *Tecnologías de la Información y la Comunicación*, sin embargo, algunos autores agregan el término "nuevas"[37] para diferenciarlas de tecnologías generadas en el pasado y que, a la fecha, devienen en obsoletas. En la literatura especializada es frecuente encontrar también el acrónimo ICT, que corresponde a las siglas *Information and Communications Technology*.

Coincido con Miró Llinares, quien sostiene que "[n]o existe una lista cerrada de elementos que configuran las TIC, sino que más bien con tal categoría se incluyen no sólo los que conforman los modos actuales de sistematización y transmisión de información, sino también los futuros. En todo caso, se viene admitiendo que se incluyen dentro de las TIC, tanto las redes (entre las cuales destaca Internet, pero también se incluyen las de telefonía móvil y otras redes telemáticas) como las terminales (entre las que destacan los sistemas informáticos consistentes en ordenadores personales, pero también comienza a ser un gran vehículo de comunicación las consolas) y los servicios, entre los que

36 Velasco San Martín/Velázquez, *Aspectos prácticos de los ciberdelitos y la evidencia digital*, cit., p. 38. Estos autores, además, resaltan su importancia y trascendencia al recordar que el 21 de diciembre de 2001, la Asamblea General de las Naciones Unidas adoptó la Resolución A/RES/56/183 que refrenda la organización de la Cumbre Mundial sobre la Sociedad de la Información conocida como WSIS, por sus siglas en inglés.

37 Díaz Colchado, Juan y Andreé Castro Arequipeño. "Los derechos fundamentales y las nuevas tecnologías de la información y comunicación: Una aproximación". En: *Thémis* 79. Lima: 2021, p. 16.

destacan todavía la descarga de archivos en sitios de intercambio y en webs de pago, pero también el comercio electrónico, la banca electrónica, la realización electrónica de actividades relacionadas con la Administración Pública y, cada vez más, las redes sociales. En todo caso, los datos personales y el patrimonio son, especialmente, los principales objetos de los servicios en la Red"[38] [sic].

De este modo, a partir de una concepción amplia, por TIC se entiende el conjunto de tecnologías que permiten recolectar, almacenar, procesar y transmitir información. Esta definición comprende las redes, las terminales y los servicios, pues son tipos de tecnologías. Además, es importante advertir sus funciones: recolección (reunión y medición), almacenamiento (registro y preservación), procesamiento (filtro y análisis) y transmisión (transferencia) y objeto (información, datos).

Ahora bien, según el *Informe sobre Desarrollo Humano en Venezuela*, elaborado en el 2002 por el Programa de las Naciones Unidas para el Desarrollo, las TIC surgen de la unión de dos expresiones *Tecnologías de la Información* y *Tecnologías Convencionales de Comunicación*. La primera es empleada para referirse a la informática, telemática o teleinformática. La segunda es, por esencia, rígida, pues sus funciones son constantes y están congeladas en el diseño de los dispositivos-[39].

En el mencionado informe se destacan algunas características de las TIC[40]:

a. Adaptables: los bienes o servicios se adecúan en función de las especificaciones de los requerimientos.

b. Convergentes: es posible compatibilizar un gran número de dispositivos.

c. Diversas: se refleja tanto en el sustrato estructural como cultural.

d. Vinculantes: facilitan la interacción comercial y social entre proveedores y consumidores.

38 Miró Llinares, *El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio*, cit., p. 25.

39 Programa de las Naciones Unidas para el Desarrollo. *Informe sobre Desarrollo Humano en Venezuela 2002. Las tecnologías de la información y la comunicación al servicio del desarrollo*, pp. 49 y s. https://hdr.undp.org/system/files/documents/venezuela2002es.pdf

40 *Loc. cit.*

e. Globalizantes: trascienden las barreras lingüísticas y culturales.

f. Penetrantes: se encuentran conectadas a ámbitos personales, profesionales y gubernamentales.

g. Permiten la creación de redes: el valor de las redes dependerá de los nodos que se generan.

h. Virtualizantes: permiten modelar el mundo físico a partir de innovaciones virtuales.

i. Habilitadoras de la eficiencia: reduce los costos de las transacciones.

j. Nivelantes: al no requerir espacios físicos, permite interacciones simultáneas que superan la distancia.

k. Autocatalíticas: el crecimiento es acelerado y estimula el ingreso de más usuarios. De este modo, una masa crítica de consumidores estimula mayores innovaciones y, a su vez, inversión en infraestructura.

Con la finalidad de graficar las características que acompañan a las cuatro generaciones que integran el tránsito de las TIC, la especialista mexicana Paola De la Rosa Rodríguez elaboró el siguiente cuadro ilustrativo[41]:

Generación	Décadas	Aparatos en uso
Primera generación. Aparatos de comunicación	Entre 1907 y 1930	Radio de amplitud modulada, reducida cobertura radiofónica, bajo consumo electrónico, etc.
Segunda generación. Medios de comunicación electrónicos	Entre 1940 y 1950	Televisión color, aparatos portátiles, radio en frecuencia modular, mayor cobertura radiodifusora, aumento del tiempo de exposición a los medios, cambios en los contenidos de programación, etc.
Tercera generación. Medios de comunicación	Entre 1950 y 1990	Cablevisión, satélites, videodisco, teletexto, computadoras, sistemas de video con enorme cobertura y gran *rating* de audiencia, rápido flujo de programación, gran versatilidad de ubicación, etc.
Cuarta generación. Tecnologías de información.	De 1990 al siglo XXI	El surgimiento de internet y sus fenómenos interactivos derivados, gradualmente transforma la estructura cultural y comunicativa anterior dando origen a un nuevo modelo de comunicación virtual que produce nuevas facetas del Estado Ampliado.

Cuadro 1: Generaciones que integran el tránsito de las TIC.

41 De La Rosa Rodríguez, Paola Iliana. *Las tecnologías, el ciberespacio y el derecho penal. Estudios sobre la prueba científica y la prueba electrónica*. Ciudad de México: Porrúa, 2019, p. 37.

1.3.2. El impacto positivo de las TIC

En el Perú, según las *Estadísticas de las Tecnologías de Información y Comunicación en los Hogares*, en el primer trimestre de 2024, el 96 % de los hogares del país tiene al menos una TIC. De este informe, extraigo algunas cifras relevantes[42]:

- En el primer trimestre de 2024, el 8,2 % de los hogares accedieron a telefonía fija. La tendencia a la baja es palpable: 2019, 23,3 %; 2020, 20,9 %; 2021, 13,4 %; 2022, 13,4 %; 2023, 10,7 %.
- En este periodo, en el 95,3 % de los hogares del país existe al menos un miembro del hogar con un teléfono celular.
- En el intervalo en referencia, el 87,2 % de hogares del país tienen únicamente teléfono celular, el 8,1 % tiene teléfono fijo y celular, el 0,1 % tiene solo teléfono fijo, mientras que el 4,6 % de los hogares no cuentan con ninguno de ellos.
- Con relación al servicio de internet, el 57,6 % de los hogares disponen de este servicio: el 77,5 % en Lima Metropolitana, el 61,3 % en el resto urbano y el 18,1 % en los hogares del área rural.
- De todos los hogares que tienen al menos una computadora, el 90,9 % es para uso exclusivo del hogar, es decir para actividades académicas, profesionales o de estudio; el 8,8 % combina su uso para el hogar y el trabajo; y el 0,4 % lo usa exclusivamente para el trabajo.
- El 71,5 % de los hogares dispone de solo una computadora, mientras que el 28,5 % cuenta con dos o más.
- El 77,7 % de la población de 6 o más años usa internet. El aumento es significativo en este quinquenio: 2019, 54,8 %; 2020, 60,5 %; 2021, 67,4 %; 2022, 72,7 %; 2023, 75 %.
- Los grupos de edad que más usan internet son los jóvenes de 19 a 24 años (95,4 %), seguidos por los de 25 a 40 años (91,4 %) y

42 Instituto Nacional de Estadística e Informática. Informe Técnico N.º 02 – Junio de 2024, *Estadística de las Tecnologías de Información y Comunicación en los Hogares. Trimestre: Enero-Febrero-Marzo 2024*. https://cdn.www.gob.pe/uploads/document/file/6543264/5702640-las-tecnologias-de-informacion-y-comunicacion-en-los-hogares-ene-feb-mar-2024.pdf

los de 12 a 18 años (86,2 %). En contraste, solo el 47,5 % de las personas mayores de 60 años accede a internet.

- En el periodo analizado, del total de usuarios de internet, el 90,7 % de la población de 6 a más años, hace uso diario. Esta cifra es interesante muestra un gran incremento al compararla con la frecuencia diaria al 2019: 78,8 %. Actualmente, el 90,4 % de hombres y el 91 % mujeres acceden a internet una vez al día.

Ahora bien, en cuanto a las actividades que realiza la población usuaria de internet, resulta interesante destacar lo siguiente:

Actividades	Total	Sexo		Grupo de edad	
		Hombre	Mujer	6 a 24 años	25 y más años
Comunicarse (e-mail, chat, llamadas por Skype, WhatsApp, Facebook, Twitter, etc.).	91,7	90,8	92,5	80,8	98,2
Obtener información	79,7	79,9	79,5	77,4	81,1
Actividades de entretenimiento (juego de video, obtener películas, música, videos, escuchar radio, leer periódico, etc.).	92,1	93,0	91,2	95,8	89,9

Cuadro 2: Actividades que realiza la población usuaria de internet, al primer trimestre de 2024[43].

No cabe duda de que el impacto de las TIC en diversos aspectos de nuestra vida ha sido altamente positivo, hasta el punto de volverse indispensable en muchos casos. A continuación, mencionaré algunos ejemplos que claramente grafican su presencia a nivel industrial, social, educativo y judicial.

1.3.2.1. A nivel industrial

El Consejo de la Agenda Global del Foro Económico Mundial sobre el Futuro del Software y la Sociedad Global encuestó a 800 ejecutivos a fin de comprender las implicaciones de las tecnologías innovadoras sobre los individuos, las organizaciones, el gobierno y la sociedad[44]. El informe *Deep Shift. Technology Tipping Points and Social Impact* fue publicado en setiembre del 2015, siendo los puntos más resaltantes los expuestos en el siguiente cuadro -el cual refleja la percepción que tenían los encuestados hace diez años-:

43 *Ibidem*, p. 12.

44 Schwab, Klaus. *La cuarta revolución industrial.* 8.ª reimpresión, Barcelona: The Penguin Random House, 2023, p. 149.

	Puntos de inflexión: ¿Qué ocurrirán antes de 2025?	Porcentaje
1.	El 10 % de las personas usarán ropa conectada a internet.	91,2 %
2.	El 90 % de la gente tendrá almacenamiento ilimitado y gratuito (patrocinado mediante publicidad).	91 %
3.	Un billón de sensores estará conectados a internet.	89,2 %
4.	Primer farmacéutico robótico en Estados Unidos.	86,5 %
5.	El 10 % de las gafas de lecturas estarán conectadas a internet.	85,5 %
6.	El 80 % de las personas tendrán presencia digital en internet.	84,4 %
7.	El primer automóvil impreso en 3D estará en producción.	84,1 %
8.	Primer gobierno que sustituirá su censo poblacional por uno basado en el Big Data.	82,9 %
9.	Primer teléfono móvil implantable disponible comercialmente.	81,7 %
10.	El 5 % de los productos de consumo estarán impresos en 3D.	81,1 %
11.	El 90 % de la población utilizará teléfonos inteligentes.	80,7 %
12.	El 90 % de la población tendrá acceso a internet.	78,8 %
13.	Los automóviles sin conductor serán el 10 % de todos los vehículos de carreteras de Estados Unidos.	78,2 %
14.	Primer trasplante de un hígado impreso en 3D.	76,4 %
15.	El 30 % de las auditorías corporativas serán realizadas mediante inteligencia artificial.	75,4 %
16.	Primera vez que un gobierno recaudará sus impuestos utilizando blockchain.	73,1 %
17.	Más del 50 % del tráfico de internet en los hogares será para electrodomésticos y dispositivos.	69,9 %
18.	En general, habrá más viajes en vehículo compartido que en coches privados.	67,2 %
19.	Primera ciudad con más de 50 000 personas que no tendrá semáforo.	63,7 %
20.	El 10 % del producto interior bruto global se almacenará con tecnología blockchain.	57,9 %
21.	Primera máquina de inteligencia artificial en una junta directiva.	45,2 %

Cuadro 3: Puntos de inflexión que ocurrirá antes de 2025[45].

Si está leyendo esta obra en el 2025, algunas predicciones se cumplieron, mientras que otras están en ese camino. En relación con el primer punto, hoy en día existe la *internet wearable* o ropa inteligente. Por ejemplo, la empresa Sensoria lanzó las Smart Running Sneakers que incorporan la IA en la suela para detectar el impacto del pie en el suelo[46]. En la misma línea, Levis Straus promociona

45 El cuadro es una adaptación de la elaborada por Klaus Schwab, quien la diseñó a partir de "Deep Shift. Technology Tipping Points and Social Impact, Consejo de Agenda Global sobre el Futuro del Software y la Sociedad, Foro Económico Mundial, setiembre de 2015" (Schwab, *La cuarta revolución industrial,* cit., pp. 43 y s.). Los veintiún puntos han sido desarrollados en el apéndice de la obra en referencia.

46 https://www.sensoriafitness.com/footwear/

su clásica casaca diseñada con tela inteligente Jacquard que permite manipular el celular y vibra, por ejemplo, cuando llega el servicio de Uber requerido[47].

No cabe duda de que el resto de los puntos de inflexión descritos son palpables: en el 2023, se presentaron las Apple Vision Pro, gafas que combinan la realidad aumentada y la realidad virtual[48]. El mismo año se publicó un informe que posiciona las cinco ciudades más inteligentes o *smart cities* del mundo: (1°) Zurich, Suiza, (2°) Oslo, Noruega, (3°) Canberra, Australia, (4°) Copenhague, Dinamarca y (5°) Lausanne, Suiza. ¿Por qué se consideran ciudades 4.0? Porque, entre otras características, gestionan grandes volúmenes de datos, monitorean en tiempo real el consumo de energía mediante circuitos interconectados, utilizan las TIC para optimizar la gestión de residuos, y emplean dispositivos tecnológicos tanto para garantizar la seguridad pública como para fortalecer la ciberseguridad[49].

1.3.2.2. A nivel social

Las TIC, especialmente a través de las redes sociales, han permitido encontrar y reencontrar amigos, familiares, compañeros de escuela o de trabajo. La primera plataforma que tuvo esta finalidad no fue *Facebook*, ya que fue creada en el 2004. Para identificar el origen de las redes sociales, debemos remontarnos una década atrás:

- *Geocities* (1994), una ciudad compuesta por diferentes barrios agrupados temáticamente.
- *Classmates* (1995), una plataforma que permitía encontrar viejos compañeros del colegio, instituto o universidad.
- *SixDegrees* (1997), plataforma que se inspiró en la teoría de los seis grados de Duncan Watts, según el cual, sin importar de qué ciudad o país sean, dos personas siempre estarán conectadas por no más de cinco intermediarios.

47 "La casaca inteligente de Google y Lev's: ¿una innovación útil?", en *Gestión*, 21 de marzo de 2017. https://gestion.pe/tendencias/casaca-inteligente-google-levi-s-innovacion-util-131231-noticia/#google_vignette

48 https://www.apple.com/apple-vision-pro/

49 Repsol. *Las ciudades inteligentes son una realidad*. [2023] https://www.repsol.com/es/energia-futuro/tecnologia-innovacion/smart-cities/index.cshtml

En el 2001, en el marco de las Jornadas sobre Gestión en Organizaciones del Tercer Sector que se celebraron en la Universidad Di Tella de Buenos Aires, se propuso la definición de redes sociales que se mantiene vigente[50]:

> Las redes son formas de interacción social, definida como un intercambio dinámico entre personas, grupos e instituciones en contextos de complejidad. Un sistema abierto y en construcción permanente que involucra a conjuntos que se identifican en las mismas necesidades y problemáticas y que se organizan para potenciar sus recursos.

Ahora bien, ¿qué está pasando en nuestro país? De acuerdo con la Agencia de Marketing Digital especializada en Campañas de Publicidad, Lima Retail, las redes sociales más usadas en Perú, al 2024, fueron las siguientes: (1) Facebook, (2) Instagram, (3), TikTok, (4) YouTube y (5) LinkedIn. Algunos datos muy interesantes sobre el comportamiento del peruano frente a estas plataformas[51]:

- A enero del 2024, el alcance de los anuncios en Facebook en Perú equivalía al 93,3 % de la base local de usuarios de internet. En este periodo, el 48,2 % de la audiencia publicitaria de Facebook en Perú eran mujeres, mientras que el 51,8 % eran hombres.
- El alcance publicitario potencial de Instagram en Perú aumentó en 1,5 millones (17,6 %) entre enero de 2023 y enero de 2024.
- El alcance publicitario potencial de TikTok en Perú aumentó en 5,0 millones (29,9 %) entre principios de 2023 y principios de 2024.
- A diferencia de YouTube que se mantuvo sin variaciones significativas, el tamaño de la audiencia publicitaria de LinkedIn en Perú aumentó en 400 mil (4,7 %) entre octubre de 2023 y enero de 2024.

Como se puede apreciar, el impacto de las principales redes sociales en Perú va en aumento, siguiendo la tendencia mundial. Este crecimiento genera

50 Gutiérrez de Aizpuru, Julia. "Implicaciones legales de las redes sociales". En: Estévez, José (dir.). *Derecho digital*. Navarra: Thomson Reuters / Aranzadi, 2019, p. 233.

51 El estudio titulado "Redes Sociales más usadas en Perú (Febrero 2025)" se encuentra disponible en: https://limaretail.com/redes-sociales/estadisticas-redes-sociales

muchos beneficios y oportunidades de negocio -a través del comercio *online*-, laborales -con la aparición de nuevas ocupaciones como el *gestor de comunidades* o el *generador de contenidos*- y educativas. Lamentablemente, también representan oportunidades para nuevas modalidades delictivas.

1.3.2.3. A nivel educativo

No cabe duda de que las TIC han facilitado el proceso de enseñanza y aprendizaje, permitiendo desde la búsqueda de información, la redacción y el procesamiento de datos hasta la implementación de clases híbridas o virtuales. Sin embargo, persisten brechas tecnológicas -ya que no todas las ciudades cuentan con el mismo acceso a internet- y brechas generacionales, pues la diferencia de edad entre docentes y estudiantes influye en la frecuencia y la forma en que utilizan estas tecnologías:

Generación	Año de nacimiento	Rango edad, al 2024
Generación Z	Desde 1996	Hasta 28 años
Generación Y (Millenials)	Entre 1980 y 1995	Entre 29 y 44 años
Generación X	Entre 1966 y 1979	Entre 45 y 58 años
Baby boomers	Entre 1945 y 1965	Entre 59 y 79 años

Cuadro 4: Años de nacimiento de las generaciones[52]. Elaboración propia.

La generación Z es denominada también "Generación V (por virtual), Generación C (por comunidad o contenido), Generación de Internet o incluso Generación Google, cuyas características comunes son el uso de las tecnologías de la información y comunicación (TIC)"[53]. La estrecha relación entre los estudiantes y las TIC no puede ser ignorada por el docente. Diversos estudios dan cuenta de este problema: "Los estudiantes que ingresan a las universidades son

52 Los años de edad fueron tomados de Duffy, Bobby. *El mito de las generaciones. Por qué cuándo naciste importa menos de lo que piensas.* Madrid: Urano, 2022, p. 27. El autor señala que no hay acuerdo total sobre dónde termina una generación y dónde empieza otra, sobre todo lo que respecta a las generaciones Z e Y. En el primer caso, algunos los sitúan entre 1996 y 2010, otros desde 1997 y los restantes desde el 2000.

53 Fernández-Cruz, Francisco José y María José Fernández Díaz. "Los docentes de la Generación Z y sus competencias digitales". En: *Comunicar. Revista Científica de Comunicación y Educación* N.º 46, 2016, p. 98. https://www.revistacomunicar.com/index.php?contenido=detalles&numero=46&articulo=46-2016-10

muy distintos a los jóvenes de generaciones anteriores, en los cuales los sistemas educativos fueron diseñados para otro tipo de estudiantes"[54]. Así, frente a estudiantes *nativos digitales*, tenemos profesores *inmigrantes digitales* -realidad que los docentes del siglo XXI no podemos ignorar[55]-.

Ahora bien, la enseñanza, especialmente la universitaria, es un *proceso intencionado* que recae en un *grupo social diferenciable*. Analicemos estas premisas para comprender sus alcances, límites y el impacto recibido por el uso masivo e intenso de las TIC:

a) Es un *proceso*, pues reúne una interacción permanente y necesaria entre el profesor (enseñanza) y el alumno (aprendizaje). Así, si bien puede existir aprendizaje sin enseñanza -piénsese en las personas autodidactas-, no se concibe la enseñanza sin el aprendizaje.

b) Es *intencionado*, porque tiene un propósito previsto o delimitado por el docente. De esta manera, la planificación es tan importante -ya que los objetivos no se improvisan- que nutre directamente esta definición.

c) Recae en un *grupo social diferenciable*. ¿Qué distingue enseñar a universitarios que a profesionales? En ambos casos nos referimos a dos tipos de educación de adultos, sin embargo, los primeros buscan competencias útiles para insertarse en el campo laboral o social, mientras que los segundos persiguen perfeccionarlas.

Ahora bien, la enseñanza evoluciona y esto trae diversos cambios. Así, por ejemplo, se considera que "frente a una concepción centrada en la enseñanza y la exposición de contenidos", se requiere que nos aproximemos a "un planteamiento docente centrado en la calidad de lo que el estudiante hace: aprendizaje

54 González Bello, Edgar Oswaldo y Adolfo Castillo Navarro. "La enseñanza universitaria en derecho con el uso didáctico de las TIC". En: *Dike, Revista de Investigación en Derecho y Criminología*, 2016, pp. 24 y s. http://www.apps.buap.mx/ojs3/index.php/dike/article/view/235

55 López Rubio, Daniel. "Twitter: Una herramienta auxiliar en la docencia del derecho constitucional". En: *Docencia y Derecho. Docencia y Derecho, Revista para la docencia jurídica universitaria* 15, 2020, p. 34. https://www.uco.es/docencia_derecho/index.php/reduca/article/viewFile/201/253

activo y constructivo para facilitar el cambio conceptual"[56]. Sin embargo, ningún fenómeno contemporáneo trajo más cambios significativos que la pandemia -de ahí que debamos identificar las oportunidades en medio de la crisis-.

Es innegable que la pandemia de COVID-19 tuvo un impacto significativo en la educación, acelerando cambios que se habían previsto desde hace décadas, como la integración y el uso de las TIC. Esto permite analizar la evolución de las instituciones educativas en tres momentos clave: antes de la pandemia, durante la crisis sanitaria y en la etapa posterior a ella.

Sobre las competencias desarrolladas en el contexto sanitario, autores como el docente mexicano José Antonio Miguel Román advertían que, mientras los estudiantes solían ser más pesimistas sobre las competencias alcanzadas, sus docentes se mostraban optimistas[57]. Esta afirmación me lleva a resaltar algunos puntos adicionales:

En primer lugar, los docentes no podemos olvidar las brechas digitales, ya que esto profundiza la desigualdad entre los estudiantes. De la misma forma, la institución a la que pertenece el docente debe saber que "existe una clara relación entre la infraestructura tecnológica de las universidades y la capacidad de resiliencia ante situaciones de emergencia que requiere aislamiento social físico"[58].

En segundo lugar, haber superado la emergencia sanitaria no nos sitúa nuevamente en el periodo anterior a la pandemia. De este modo, los avances obtenidos como la incorporación de las clases híbridas o el uso de herramientas digitales no deben ser olvidados, sino asimilados.

---

56 Paricio, Javier, Idoia Fernández y Amparo Fernández. "Una concepción de la docencia problemática, compleja y basada en la investigación". En: Paricio, Javier *et al. Cartografía de la buena docencia universitaria. Un marco para el desarrollo del profesorado basado en la investigación*. Madrid: Narcea, 2019, p. 24.

57 Miguel Román, José Antonio. "La educación superior en tiempos de pandemia: Una visión desde dentro del proceso formativo". En: *Revista Latinoamericana de Estudios Educativos*, vol. L, número especial, México: 2020, p. 12. https://www.redalyc.org/jatsRepo/270/27063237017/html/index.html

58 Tanata Vásquez, Heydi. "Educación superior en tiempos de pandemia". En: *Ciencia Latina Revista Científica Multidisciplinar 5(6)*, México: 2021, p. 11. https://ciencialatina.org/index.php/cienciala/article/view/1368/1886

En tercer lugar, en la pandemia estuvimos expuestos a copiosas pérdidas humanas y dramas sociales. Esto orilló a los docentes a ser mucho más empáticos con los alumnos al preocuparse por su bienestar. Estas cualidades personales tampoco pueden ser descuidadas al retornar a la presencialidad.

En cuarto lugar, la presencialidad y la virtualidad son experiencias distintas. De este modo, coincido con Casero Béjar y Sánchez Vera cuando sostienen que la virtualidad no es una *simulación de la presencialidad*[59]. En efecto, el docente debe capacitarse para abrir nuevas experiencias didácticas y, de ser el caso, evaluativas que se beneficien del uso de las TIC, pero debe ser consciente que no debe convertir la plataforma virtual en una copia de lo presencial.

El proceso de enseñanza/aprendizaje, a través de las TIC, exige planificación y supervisión interna -a través de los órganos de control respectivos- como externa -de las instituciones gubernamentales-. Perú inició un proceso de mejora en la educación superior; sin embargo, los avances se perdieron y, hoy en día, estamos en sentido inverso. Así, pese a la oposición y crítica por las últimas modificaciones legislativas, el Congreso de la República estableció que, salvo contadas excepciones, la enseñanza en las universidades peruanas puede ser 100 % virtual. De este modo, el 5 de agosto de 2024, se publicó la Ley N.º 32 105, Ley que modifica la Ley 30 220, "Ley Universitaria, para disponer el carácter permanente de la modalidad a distancia en la Educación Superior y afianzar su acceso". Resalto el artículo 47 por su confusa redacción:

> 47.4.1. La modalidad a distancia o no presencial se caracteriza por la interacción, ya sea simultánea o diferida, entre los estudiantes y los docentes, facilitada por medios tecnológicos que promuevan el aprendizaje autónomo. Esta modalidad podrá comprender hasta el 100 % de los créditos académicos, siempre y cuando se utilicen tecnologías de información y la comunicación (TIC) certificadas, excepto para las carreras y especialidades que requieran realización de experimentos y prácticas presenciales. **Este proceso deberá complementarse con convenios tipo google, internet e inteligencia artificial** [El resaltado es mío].

59 Casero Bejar, María y María Sánchez Vera. "Cambio de modalidad presencial a virtual durante el confinamiento por COVID-19: percepciones del alumnado universitario". En: *RIED, Revista Iberoamericana de Educación a Distancia*, 25(1), Madrid: 2022, p. 257. https://www.redalyc.org/journal/3314/331469022015/331469022015.pdf

47.4.2. Los mecanismos para garantizar la calidad de la modalidad a distancia son los siguientes:

a) Plataforma de gestión académica virtual. Consiste en la implementación de plataformas de gestión académica que permitan la interacción continua entre docentes y estudiantes, con herramientas para seguimiento, evaluación y retroalimentación.

b) Estándares de calidad para TIC. Consiste en la definición de estándares de calidad para las TIC utilizadas en la educación a distancia, asegurando su efectividad y accesibilidad.

c) Capacitación continua. Comprende programas de capacitación continua para docentes en el uso de las TIC y los métodos pedagógicos adaptados a entornos virtuales.

d) Evaluación de satisfacción. Encuestas periódicas a estudiantes y docentes para evaluar la satisfacción y efectividad de la modalidad a distancia, con mecanismos para implementar mejoras basadas en los resultados.

Imagino que el lector, al igual que yo, no comprende lo que el legislador peruano intentó expresar al señalar que "este proceso deberá complementarse con convenios tipo google, internet e inteligencia artificial". Al margen del desenfreno legislativo que no solo gobierna el ámbito penal sino, como vemos, todo ámbito social, nadie puede dudar de los beneficios que traen las TIC para la educación[60]. No obstante, finalizo esta breve reflexión señalando que, si bien existe una brecha generacional entre el docente y el alumno, esa brecha es mucho más grande entre la legislación y la educación, en lo que al uso de las TIC se refiere.

1.3.2.4. A nivel judicial

Actualmente, los litigantes peruanos podemos participar en una declaración testimonial en una sede fiscal en Tumbes por la mañana y, por la tarde,

60 Por ejemplo, sobre el uso de la IA en la educación, el Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado (INTEF) del Ministerio de Educación, Formación Profesional y Deportes de España publicó, en el 2024, la "Guía sobre el uso de la Inteligencia Artificial en el ámbito educativo". https://code.intef.es/wp-content/uploads/2024/07/Guía-sobre-el-uso-de-la-IA-en-el-ámbito-educativo-INTEF_2024.pdf

en un juicio oral en Tacna, a pesar de que ambas ciudades están separadas por 2 508 kilómetros —un recorrido de 39 horas en auto sin pausas—. Esto es posible gracias a las TIC y a las políticas implementadas por el Ministerio Público y el Poder Judicial.

En efecto, el uso de las TIC ha posibilitado desde la realización de diligencias de forma remota hasta la celebración de importantes juicios orales, a través de Google Meet, sin que se afecten los principios de inmediación, contradicción y publicidad, tal y como lo reconoció el Tribunal Constitucional en la STC del 30 de julio de 2015, recaída sobre el Exp. N.º 02738-2014-HC/TC[61].

Como recuerda el procesalista Reyna Alfaro[62], en Perú, antes de la pandemia, se emitieron importantes normas que maximizaron el uso de las TIC: **(i)** Directiva N.º 001-2013-CE-PJ, procedimiento para la ejecución de audiencias virtuales, **(ii)** Art. 119-A CPP[63], incorporada mediante la Ley N.º 30076, que reconoce la posibilidad excepcional de la presencia virtual del acusado en juicio y **(iii)** Directiva N.º 001-2014-CE-PJ, lineamientos para el uso de la videoconferencia en los procesos penales.

El periodo de aislamiento obligatorio no podía retrasar o impedir que el sistema de administración de justicia avance, por lo que se implementó un

61 "A juicio de este Tribunal, el sistema de videoconferencia no impide que el procesado y el juzgador puedan comunicarse oralmente; antes bien, posibilita la interacción y el dialogo entre las partes, pudiéndose observar que cuando se realiza bajo las condiciones técnicas adecuadas no obstaculiza la mejor percepción sensorial. Asimismo, en la medida que se permita el acceso al contenido de las audiencias no se afecta la publicidad. Mientras que, respecto de la contradicción, se aprecia que con las partes comunicadas en tiempo real, estas pueden expresarse fluidamente, tal y como si estuvieran presentes físicamente el procesado y el juzgador en el mismo ambiente" (Exp. N.º 02738-2014-HC/TC, F. J. 18).

62 Reyna Alfaro, Luis. "Litigación y persuasión *on streaming*. Una aproximación a los retos de la justicia virtual". En: *Gaceta de Litigación Penal* 3, noviembre-diciembre. Lima: 2021, pp. 95-106.

63 **CPP, art. 119-A. *Audiencia.*** 1. La presencia física del imputado es obligatoria en la audiencia del juicio, conforme al inciso 1) del artículo 356, así como en aquellos actos procesales dispuestos por ley.
2. Excepcionalmente, a pedido del fiscal, del imputado o por disposición del juez, podrá utilizarse el método de videoconferencia en casos que el imputado se encuentre privado de su libertad y su traslado al lugar de la audiencia encuentre dificultades por la distancia o porque exista peligro de fuga.

marco normativo que lo agilizó: **(i)** Protocolo denominado "Medidas de reactivación de los órganos jurisdiccionales y administrativos del Poder Judicial, posterior al levantamiento del aislamiento social obligatorio", **(ii)** Resolución Administrativa N.° 000123-2020-CE-PJ que autorizó el uso de Google Hangouts Meets para la comunicación de abogados y litigantes con los jueces, **(iii)** Resolución Administrativa N.° 000173-2020-CE-PJ que aprobó el protocolo temporal para audiencias virtuales durante el periodo de emergencia sanitaria y **(iv)** Resolución Administrativa N.° 00025-2021-CE-PJ que prorrogó la vigencia de las primeras citadas; entre otras.

Lamentablemente, no todos los litigantes están familiarizados con el uso de las TIC, ni se han realizado estudios institucionales que permitan evaluar su impacto positivo o negativo en la administración de justicia. ¿Cuál será el futuro? A pesar de que aún no se ha consolidado el uso de herramientas básicas ni se ha capacitado adecuadamente al personal administrativo en seguridad informática, ya se promueve la implementación de la inteligencia artificial y el expediente electrónico judicial. Si bien estas iniciativas son valiosas, en el contexto peruano es fundamental avanzar de manera progresiva y con bases sólidas, garantizando primero una adecuada formación y seguridad en el sistema.

1.3.3. El impacto negativo de las TIC: facilitan la comisión de delitos y crean otros tantos

Líneas atrás indiqué que el art. 1 LDI precisa que el objeto de la ley es sancionar las conductas cometidas mediante el uso de las TIC. En la versión original de la ley, los siguientes delitos incluían las TIC como elementos objetivos del tipo: Atentado a la integridad de datos informáticos (art. 3 LDI), atentando a la integridad de sistemas informáticos (art. 4 LDI), proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos (art. 5 LDI), interceptación de datos informáticos (art. 7 LDI), fraude informático (art. 8 LDI) y suplantación de identidad (art. 9 LDI).

Sin embargo, en marzo de 2014, se eliminó toda referencia a las TIC en los tipos penales previstos en los art. 3, 4, 5, 7 y 8 LDI dejando incólume la mención de los arts. 1 y 9 LDI. Si bien los proyectos de ley no explicaron el motivo de la eliminación, en el diario de debates sí se abordó el tema. El motivo: "evitar" excesos punitivos.

> El señor Guevara Amasifuen (AP-FA) – Gracias, presidente; colegas congresistas, buenas tardes.
>
> El tema que hoy estamos debatiendo es un tema que debemos actuar con absoluta prudencia, yo diría como casi equilibrista, en qué sentido, en el sentido de que debemos de proteger diversos factores y actores, precisamente lo que aquí se está buscando delitos de pornografía, el tema relacionado de acoso, el tema de discriminación incluso, sin embargo, en la otra parte encontramos que debemos ser cuidadosos en que no cometamos excesos en lo que es tema de llevar a lo que es hacer que la Internet no sea libre; por lo tanto, aquí debemos tener mucho cuidado. Aquí se está denunciando y se está invocando incluso al Convenio de Budapest [sic].
>
> El Convenio de Budapest no dice textualmente todo lo que nosotros aquí debemos estar cuidando.
>
> A mí me preocupa mucho, y es por eso que invoco a la reflexión y al presidente de la Comisión de Justicia, de que busquemos que **no cometamos excesos**, por ejemplo, en el tema de lo que significa transgredir la libertad y **cometamos una cierta abolición de la libertad a lo que se refiere al uso de la tecnología, información y comunicación.**
>
> [...]
>
> Por otro lado también, es importante, como reitero, de que **veamos que el uso de tecnología, información y comunicación** no caiga o se exceda en lo que se refiere al delito informático [El resaltado es mío].

Finalmente, el delito de suplantación de identidad fue modificado en diciembre del 2023, variándose el término "mediante las tecnologías de la información o comunicación" por "mediante las tecnologías digitales". En la exposición de motivos del Decreto Legislativo N.º 1591 se explica la razón del cambio: homologar su significado con el previsto en la ley de gobierno digital y, de este modo, incluir la inteligencia artificial como medio comisivo:

> Así pues, los cambios propuestos consisten en actualizar el término "tecnologías de información o de comunicación" por "tecnologías digitales" que incluye el uso de tecnologías emergentes como la inteligencia artificial, conforme al Decreto Legislativo N.º 1 412, Ley del Gobierno Digital:

> **Artículo 3.- Definiciones**
>
> Para efectos de la presente Ley, se adoptan las siguientes definiciones:
>
> 1. Tecnologías digitales.- Se refieren a las Tecnologías de la Información y Comunicación – TIC, incluidos internet, las tecnologías y dispositivos móviles, así como la analítica de datos utilizados para mejorar la generación, recopilación, intercambio, agregación, combinación, análisis, acceso, búsqueda y presentación de contenido digital, incluido el desarrollo de servicios y aplicaciones a la materia de gobierno digital.

Considero que en muy poco tiempo el elemento TIC regresará a los tipos penales que integran la LDI, porque en diciembre del 2024 se aprobó la Convención de las Naciones Unidas contra la ciberdelincuencia, titulado "Fortalecimiento de cooperación internacional para la lucha contra determinados delitos cometidos mediante sistemas de tecnología de la información y las comunicaciones y para la transmisión de pruebas en forma electrónica de delitos graves"[64]. En este cuerpo normativo, se recogen las TIC como elementos objetivos del tipo. Así, basta con observar la redacción de dos artículos, a modo de ejemplo:

> **Art. 7. Acceso ilícito.**
>
> Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para tipificar como delito en su derecho interno el acceso deliberado y sin derecho a la totalidad o parte de un sistema **de tecnología de la información y las comunicaciones** [El resaltado es mío].

64 En la Convención, el elemento TIC se encuentra presente en el delito de acceso ilícito (art. 7), interceptación ilícita (art. 8), interferencia con un sistema de tecnología de la información y comunicación (art. 10), uso indebido de dispositivos (art. 11), robo o fraude relacionados con un sistema de tecnología de la información y la comunicación (art. 13), delitos relacionados con material en línea que muestra abusos sexuales de niños o explotación sexual de niños (art. 14), instigación o captación con el fin de cometer un delito sexual contra un niño (art. 15), difusión no consentida de imágenes de carácter íntimo (art. 16).

> **Art. 10. Interferencia con un sistema de tecnología de la información y las comunicaciones**
>
> Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para tipificar como delito en su derecho interno la obstaculización grave, deliberada y sin derecho del funcionamiento de un sistema de **tecnología de la información y las comunicaciones** mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos electrónicos [El resaltado es mío].

Así como destaqué los beneficios de las TIC, es indudable que los delincuentes también las emplean en actividades ilegales, ya que tratan de aprovechar el anonimato que les proporciona, la dificultad de la investigación por los escasos conocimientos o recursos tecnológicos de los aparatos estatales, la volatilidad de la prueba digital, entre otros. Si bien en el siguiente apartado describiré diversos tipos de ciberataques y los graficaré con ejemplos que permitirán comprender el impacto de la ciberdelincuencia en nuestras vidas, es importante que el lector conozca algunos estudios globales[65]:

- En 2023, los ataques de *ransomware*, la explotación sexual infantil y las estafas en línea fueron las amenazas más frecuentes en la Unión Europea. El panorama fue diverso y comprendió tanto atacantes que actuaban de forma individual como redes criminales.
- Los marcos regulatorios de la UE se están actualizado y adaptando para fortalecer y proteger los sistemas informáticos y, de esta forma, hacer que la experiencia del usuario sea segura. Sin embargo, el factor humano sigue siendo el eslabón más débil en la mayoría de los escenarios.

65 Los datos compartidos fueron extraidos de (1) European Union Agency For Law Enforcement Cooperation. *Internet Organised Crime Threat Assessment (IOCTA) 2024*. Luxemburgo: Publications Office of the European Union, 2024. https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024 (2) Internet Crime Complaint Center. *Federal Bureau of Investigation: Internet Crime Report 2023*. https://www.aha.org/system/files/media/file/2024/03/fbi-internet-crime-report-2023.pdf (3) Centro De Política Y Derecho De Ciberseguridad Y Universidad De Duke. *Preparación cibernética en los sectores públicos de América Latina: Lecciones de la primera línea*. LATAM CISO Report, 2024. https://es.weforum.org/stories/2024/05/lecciones-de-ciberseguridad-de-la-batalla-de-america-latina-contra-las-amenazas-de-ransomware/

- La dinámica del mercado criminal relacionada al *malware* y a los servicios de *phishing* se asemeja a la dinámica de industrias o compañías legítimas, en tanto que el comercio de datos robados se está convirtiendo en la principal amenaza relacionada con el crimen como servicio (CaaS).
- La *dark web* continúa siendo un facilitador clave para los ciberdelincuentes, pues permite compartir conocimiento, herramientas y servicios de manera subrepticia. Además, TOR sigue siendo la plataforma más popular para su acceso.
- El uso de criptomonedas en diferentes áreas de la ciberdelincuencia se ha vuelto evidente, destacando el Bitcoin como la criptomoneda más utilizada. Asimismo, la banca subrepticia u oculta para el lavado de criptoactivos parece estar en aumento.
- El Internet Crime Complaint Center (IC3) del FBI, en el 2023, recibió 880 418 quejas (denuncias) por 12,5 billones de dólares en pérdidas. Para representarnos el incremento anual, veamos las cifras del 2019: 467 361 quejas (denuncias) por 3,5 billones de dólares.
- Los cinco ataques más frecuentes reportados ante el IC3, en el 2023, fueron: *phishing* (298 878 quejas), personal data breach (55 851), *non-Payment/non-Delivery* (50 523), extorsión (48 223) y *tech support* (37 560).
- Las pérdidas denunciadas ante el IC3, en el 2023, producidas por los fraudes de inversión se incrementaron significativamente. De un lado, las falsas inversiones aumentaron de 3,31 billones de dólares en el 2022 a 4,57 billones de dólares en el 2023. De otro, las falsas inversiones en criptomonedas pasaron de 2,57 billones de dólares en el 2022 a 3,96 billones al año siguiente.
- Según el Banco Interamericano de Desarrollo (BID) solo siete (7) de los 32 países latinoamericanos tienen planes para proteger su infraestructura crítica de posibles ciberataques. De ellos, solo 20 cuentan con Equipos de Respuesta a Incidentes de Seguridad Cibernética (CSIRT).
- El costo anual de los ciberataques en América Latina y el Caribe podría superar los 90 millones de dólares en 2025. Se estima en 18 millones de ataques por año.

1.4. CIBERATAQUES PUROS, RÉPLICA Y DE CONTENIDO

El Convenio sobre la Ciberdelincuencia o Convenio de Budapest es el instrumento internacional actual más importante en la lucha contra este fenómeno delictivo. Como más adelante se desarrollará, si bien fue adoptado por el Consejo de Europa en el 2001, se encuentra vigente en Perú desde diciembre del 2019. A diferencia de nuestro ordenamiento, el Convenio ordena la tipología en cuatro categorías: (i) delitos contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos, (ii) delitos informáticos, (iii) delitos relacionados con el contenido y (iv) delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines[66].

A pesar de la utilidad de la clasificación establecida en el Convenio sobre la Ciberdelincuencia, considero que el esquema propuesto por el catedrático español Miró Llinares ofrece una perspectiva más clara y estructurada para analizar el fenómeno en estudio. Su clasificación se organiza en dos ejes principales: según el uso de las TIC, distingue entre ciberataques puros, de réplica y de contenido; y según su finalidad, los categoriza en cibercrímenes económicos, sociales y políticos.

Antes de continuar, es importante destacar que la reciente Convención de las Naciones Unidas contra la Ciberdelincuencia, adoptada en diciembre de 2024, enumera once delitos informáticos sin una clasificación estructurada. Con esto en mente, pasemos a analizar la propuesta del profesor Miró Llinares:

	Ciberataques puros	Ciberataques réplica	Ciberataques de contenido
Cibercrímenes económicos	• *Hacking* • *Malware* intrusivo • *Malware* destructivo • Ataques de *insiders* • Ataques DoS • *Spam* • Ciberocupación • *Antisocial networks*	• Ciberfraudes (*phishing, pharming, scam, auction fraud...*) • *Cyberspyware* (uso de *sniffers* y demás *spyware*, ciberespionaje de empresa) • *Identity theft* • *Spoofing* (DNS *spoofing*, ARP *spoofing*, IP *spoofing*, *web spoofing*) • Ciberblanqueo de capitales • Ciberextorsión • Ciberocupación	• Distribución de pornografía infantil en internet • Ciberpiratería intelectual

66 Recomiendo el estudio comparativo sobre la tipología propuesta en el Convenio de Budapest y la desarrollada en la legislación española, abordado en: Estévez, José Francisco y Elena Santos. "Ciberdelitos y ciberseguridad". En: Estévez, José (dir.). *Derecho digital*. Navarra: Thomson Reuters / Aranzadi, 2019, pp. 367-399.

	Ciberataques puros	Ciberataques réplica	Ciberataques de contenido
Cibercrímenes sociales		• *Spoofing* • *Cyberstalking* • *Cyberbullying* • *Online harassment* (ciberamenazas, coacciones, injurias, etc.) • Sexting (y extorsión con imágenes de *sexting*) • *Online grooming*	
Cibercrímenes políticos	• Ataque DoS (*cyberwar*) • Ataque DoS (*cyberhacktivism*) • *Malware* intrusivo	• Ciberespionaje terrorista • Ciberguerra	• *Online hate speech* • Ciberterrorismo (difusión de mensajes radicales con fines terroristas)

Cuadro 5. Modalidades de cibercrimen. Elaborado por Fernando Miró Llinares.

Los diferentes tipos de ataques contenidos en el cuadro serán definidos a continuación. Además, graficaré cada ciberataque con casos reales que permitirán -espero- comprender sus alcances y que, además, el lector pueda advertir que el fenómeno es real y que se encuentra presente en nuestro quehacer cotidiano.

1.4.1. Ciberataques puros

Son aquellos delitos que surgen con la aparición del Internet y que solo pueden ser cometidos por y contra las TIC a través del ciberespacio: "Se trata, por tanto, de cibercrímenes puros, de los únicos que podrían ser denominados como tales en el caso de que la condición de pertenencia fuera que solamente deben ser posibles en el ciberespacio. Y esto es así porque en ellos las TIC no solo constituyen el medio comisivo de tales ataques, sino que son el único posible, en cuanto que son medio y objetivo, y no es posible producir la esencia de ilicitud de estas infracciones si no es en el ciberespacio"[67].

1.4.1.1. Hacking

Conocido como *intrusismo informático* o *acceso ilícito*, es un tipo de ataque por el cual el ciberdelincuente accede a un sistema informático sin contar con la autorización requerida y, por lo general, vulnerando las medidas de seguridad establecidas para salvaguardar la confidencialidad.

67 Miró Llinares, *El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio*, cit., p. 53.

[**Caso 3**] En junio del 2018, el gerente de la residencia Buenos Aires, del Ayuntamiento de Valencia de Alcántara, España, insertó un USB en el ordenador personal de una enfermera que trabajaba en el mismo centro geriátrico. Logró acceder a su contenido. Poco tiempo después, en octubre del mismo año, el gerente ingresó a la oficina de la enfermera y, sin su conocimiento o consentimiento, volvió a acceder a su ordenador navegando por sus carpetas privadas, entre ellas, algunas relacionadas a servicios de catering e, incluso, al contrato de arrendamiento de la vivienda de la víctima.

La agraviada acudió a la policía y retornó acompañada de dos agentes quienes vieron salir al gerente de la enfermería. Si bien el ordenador estaba apagado, constataron que la fuente de poder estaba caliente. Todo esto fue ratificado por un informe pericial que determinó que el 11 de octubre de 2018 se accedió al ordenador, se modificó la contraseña y se revisaron diversas carpetas personales. En el proceso, se demostró que el gerente buscaba información que pudiese perjudicar a la enfermera, pues quería el puesto para su novia. Fue condenado[68].

1.4.1.2. Malware intrusivo

Conocido como *spyware*. Es un *software* malicioso que se instala sin el consentimiento informado del usuario, se oculta en un sistema informático para controlar su actividad y obtener información confidencial como datos bancarios y contraseñas o credenciales.

[**Caso 4**] Lorenza y Pedro mantuvieron una relación sentimental hasta el 2020, pero en setiembre de ese año inician la convivencia. A fines de ese mes, tuvieron una fuerte discusión en la que Pedro le quita el celular a Lorenza. A pesar de sus esfuerzos, no logró recuperarlo de inmediato. Un par de días después, tuvieron su última discusión, marcando el final de su relación.

Lorenza sostuvo que Pedro accedía a sus conversaciones de WhatsApp para saber con quién chateaba. Así, en una ocasión, Pedro contactó a un joven

68 SAP CC 1127/2011. Sentencia N.º 276/2021 del 26 de octubre del 2021, emitida por la Audiencia Provincial de Cáceres, Sección N.º 2. Ponente: Julia Domínguez Domínguez.

con quien saldría su expareja para disuadirlo y evitar el encuentro. En este caso se barajaron dos posibilidades: Cuando Pedro le arrebató el celular le instaló un programa de *malware* espía para conocer el contenido de sus comunicaciones o para desviar sus conversaciones a un ordenador. Pedro fue sentenciado por violencia doméstica y de género[69].

1.4.1.3. Malware destructivo

Es un *software* malicioso diseñado para destruir, eliminar o borrar información de un sistema informático.

[Caso 5] Sixto trabajó para Norma 4 Servicios Informáticos S. A., a través de la cual prestó servicios a Produban hasta el 3 de marzo del 2017, en la Ciudad Financiera del Banco Santander en Boadilla del Monte, España. Creó una bomba lógica que tenía la capacidad de permanecer suspendida o inactiva por un periodo predeterminado. Así, Sixto programó que se activara el 20 de marzo de ese año. Al día siguiente, se inutilizó simultáneamente 3 168 equipos informáticos del Banco Santander en toda España. Esto afectó a 839 oficinas y generó perjuicios ascendentes a 292 237.86 euros.

En el proceso se demostró que, como consecuencia de su desvinculación, el 2 de marzo de 2017 a las 17:27:43, Sixto introdujo un código malicioso que desencadenó este ataque cibernético; sin embargo, no logró ocultar su dirección IP. Fue condenado por daños informáticos[70].

1.4.1.4. Ataques de *insiders*

Ataques dirigidos por personas que tienen o tuvieron acceso legítimo a los sistemas informáticos de la organización y que emplean sus privilegios para poner en riesgo la seguridad informática. Generalmente son empleados,

69 SAP LE 560/2024. Sentencia N.º 127/2024 del 26 de marzo del 2024, emitida por la Audiencia Provincial de León, Sección N.º 3. Ponente: Nuria Valladares Fernández.

70 STS 1008/2024. Sentencia N.º 183/2024 del 29 de febrero del 2024, emitida por la Sala de lo Penal del Tribunal Supremo de España, Sección N.º 1. Ponente: Carmen Lamela Díaz.

exempleados o proveedores. Pueden actuar de manera independiente o ser contratados por terceros para perjudicar a la institución.

[**Caso 6**] En junio de 2019, Desjardins Group -cooperativa de servicios financieros canadiense y la federación de cooperativas de ahorro y crédito más grande de América del Norte- anunció una brecha de datos que comprometió nombres, direcciones, fechas de nacimiento, números de seguro social, dirección de correos electrónicos e información acerca de los hábitos financieros de sus usuarios. Dicha brecha expuso a 2,7 millones de personas y alrededor de 173 000 empresas. El responsable fue un empleado (*insider*) que recopiló información y la compartió con un tercero que no pertenecía a su institución[71].

Tres años después, el Tribunal Superior de Quebec aprobó un acuerdo de más de 200 millones de dólares en una demanda colectiva relacionada con la brecha de seguridad y filtración de datos. En el 2024, la policía de Canadá arrestó a tres personas relacionadas con la filtración[72].

1.4.1.5. Ataques DoS

Es un tipo de ciberataque que tiene por finalidad que un sistema informático no esté disponible para los usuarios a los que va dirigido, interrumpiendo el normal funcionamiento del mismo. En general, este tipo de ataques surge cuando se inunda con solicitudes que sobrecargan el tráfico habitual, haciendo que sea incapaz de procesarlo. Esto genera una denegación de servicios.

---

71 "Un banco, un insider y los datos de 2,7 millones de personas robados", en *Panda Mediacenter*, 15 de julio de 2019. https://www.pandasecurity.com/es/mediacenter/desjardins-insider-brecha-datos/
En la misma línea: Office of the privacy commisioner of Canada. *Investigation into Desjardins' compliance with PIPEDA following a breach of personal information between 2017 and 2019*, publicado el 14 de diciembre de 2020. https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2020/pipeda-2020-005/

72 "Police arrest 3 in connection with massive Desjardins data breach", en *CBC NEWS*, 12 de junio de 2024. https://www.cbc.ca/news/canada/montreal/desjardins-data-breach-arrests-1.7232812

Cuando el ataque proviene de un solo punto de origen, se denomina *ataque de denegación de servicio* o *DoS* (*Denial of Service*). En cambio, cuando el ataque surge de varios, se conoce como *ataque de denegación de servicio distribuido* o *DDoS* (*Distributed denial-of-service*).

[Caso 7] El equipo de respuestas a ataques DDoS de Google informa que los ataques distribuidos de denegación de servicio están en aumento exponencial. Así, en junio del 2022, registraron lo que fue -a esa fecha- el mayor ataque en la historia: 46 millones de solicitudes por segundo (rps). Un año después, en octubre del 2023, una nueva serie de ataques alcanzó un pico de 398 millones de rps. Este ataque de dos minutos generó más solicitudes que el número total de visitas a artículos de Wikipedia en setiembre del 2023[73].

1.4.1.6. Spam

Conocido también como correo basura. Son los mensajes no deseados enviados por remitentes desconocidos o por, en algunos casos, remitentes falsos. Por lo general, se envían en grandes cantidades con fines publicitarios o como complemento de actividades maliciosas -por ejemplo, distribuir *malware*-.

[Caso 8] Entre el 2004 y el 2008, Luis Pablo consiguió los datos de tarjetas bancarias de múltiples ciudadanos españoles y extranjeros. Para ello utilizaba correos masivos (*spam*) que contenían páginas web duplicadas de entidades financieras. Las víctimas respondían brindando datos personales y bancarios, lo que permitió que terceros realicen operaciones fraudulentas. A través de cuentas receptoras de familiares y amigos, obtuvo 671 667 euros. Tres entidades financieras presentaron reclamos indemnizatorios: (1) Caixa, por 334 382.39 euros; (2) Bankia, por 11 240.43 euros; y (3) BBVA, por 5 780.29 euros. Luis Pablo fue condenado por estafa[74].

---

73 Kiner, Emil y Tim April, "Google mitigated the largest DDoS attack to date, peaking above 398 million rps", en *Google cloud*. 10 de octubre de 2023. https://cloud.google.com/blog/products/identity-security/google-cloud-mitigated-largest-ddos-attack-peaking-above-398-million-rps

74 SAN 6038/2023. Sentencia N.º 21/2023 del 30 de noviembre del 2023, emitida por la Sala de lo Penal de la Audiencia Nacional de España, Sección N.º 1. Ponente: Jesús Eduardo Gutiérrez Gómez.

1.4.1.7. Ciberocupación

Conocido también como apropiación de nombres de dominio o *cybersquatting*, esta conducta consiste en registrar un dominio que simula ser uno legítimo para utilizarlo con fines fraudulentos. Una modalidad muy difundida es el *typosquatting*, en el que la víctima visita una web fraudulenta al digitar o tipear de manera incorrecta el nombre. Por ejemplo, un ciberdelincuente registra el dominio **eliaspueles.com** para que los usuarios que tipeen mal mi web no visten **eliaspuelles.com**, sino la del delincuente.

[Caso 9] En el 2022, ante el creciente interés por los *token* no fungibles (NFT) o activos digitales encriptados, se detectaron más de 200 dominios con la estructura lingüística *nft* junto al nombre de diversas marcas que no ofrecen este tipo de activos o servicios[75]: paypalnft[.]com, applenft[.]com, nftcocacola[.]com, nftmcdonal[.]com, googlenft[.]com, nikenft[.]com, jpmorgannft[.]com. A menudo, esta técnica es utilizada para distribuir *malware* o lanzar campañas de *phishing*.

1.4.1.8. Antisocial networks

Conocido también como redes sociales antisociales. Los ciberdelincuentes se aprovechan o utilizan las redes sociales para el fraude u otras actividades ilícitas.

[Caso 10] Remigio, de 45 años, fue profesor de música de Dolores. La contactó a través de un perfil falso en Instagram desde que la menor tenía entre 11 y 12 años. Inicialmente, utilizó el usuario «Bigotes» y, después, «Chato». El acusado se presentó como un apoyo emocional que intentaba ayudarla. Sin embargo, poco tiempo después, le solicitó fotos de ella desnuda y videos masturbándose. Llegado el momento, Remigio le reveló su identidad, llevando la práctica virtual al abuso sexual físico.

75 Cybercrime magazine. *As NFT's Popularity Grows, So Does Cybersquatting*, publicado el 4 de febrero de 2022. https://cybersecurityventures.com/as-nfts-popularity-grows-so-does-cybersquatting/

Cuando la víctima cumplió 16 años, decidió bloquearlo de las redes sociales, exponer estos graves hechos en el colegio y denunciarlo ante la Guardia Civil. Remigio fue condenado[76].

1.4.1.9. Ciberguerra o *cyberwar*

Conocido también como *cyberwarfare*, guerra informática, guerra digital o guerra cibernética. Son los ataques cibernéticos dirigidos por un país contra otro y que buscan obtener alguna ventaja estratégica o militar.

[**Caso 11**] En medio de la guerra librada entre Ucrania y Rusia, se abrió otro frente: una batalla en el ciberespacio. Así, por ejemplo, Oleksandr, un hacker ucraniano, ayudó a desactivar temporalmente cientos de sitios web rusos, interrumpió servicios en decenas de bancos y vandalizó sitios web escribiendo mensajes a favor de su país. El Ejército TI de Ucrania está integrada por una red voluntaria de casi 200 mil usuarios en Telegram. Entre sus formas de ataque se encuentra la denegación de servicio (DoS)[77].

En el bando ruso se encuentra el grupo denominado Killnet, liderado por Killmilk, que reúne a casi 100 mil suscriptores en Telegram. Entre los ataques que se atribuyen, se encuentra una ola que desconectó temporalmente los sitios web de la OTAN y la publicación de correos electrónicos de trabajadores de la citada institución.

1.4.1.10. Ciberactivismo o *cyberhacktivism*

Conocido también como activismo en línea o activismo virtual. En principio, no es una actividad ilícita, ya que es un tipo de protesta en el que se emplean las TIC para difundir mensajes a favor de diferentes causas -benéficas, por lo general- u obtener algún resultado específico. Sin embargo, este panora-

76 SAP 430/2024. Sentencia N.º 155/2024 del 17 de julio de 2024, emitida por la Audiencia Provincial de Ourense, Sección N.º 2. Ponente: María de los Ángeles Lamas Méndez.

77 "La otra guerra inclemente que libran Ucrania y Rusia", en *BBC News Mundo*, 15 de abril de 2023. https://www.bbc.com/mundo/noticias-internacional-65266795

ma cambia cuando el medio o instrumento empleado es un delito como, por ejemplo, el secuestro informático.



Imagen 3. El grupo Anonymous hackeó diversas páginas gubernamentales y pidió a sus seguidores a unirse al movimiento #OpIndependencia[78].

[Caso 12] En julio del 2024, los sistemas informáticos de Disney fueron hackeados por un grupo denominado Nullbulge[79]. Los hacktivistas obtuvieron 1 TB de información sobre futuros proyectos, artes conceptuales y archivos internos, desde la plataforma de mensajería Slack. Los ciberatacantes sostienen que la medida se adoptó como un acto de protesta por los abusos de la compañía contra sus trabajadores, para promover los derechos de los artistas creativos y por el enfoque de Disney sobre el uso de la inteligencia artificial.

78 "Anonymous hackeó web de la Presidencia y otras páginas del Estado", en *Peru21*, Lima, 26 de agosto de 2019. https://peru21.pe/cheka/tecnologia/anonymous-hackeo-web-presidencia-paginas-117447-noticia/

79 Centro Nacional de Seguridad Digital. *Alerta integrada de seguridad digital N.º 164-2024*. Lima: 15 de julio de 2024, p. 4. https://www.gob.pe/institucion/pcm/informes-publicaciones/5785248-alerta-integrada-de-seguridad-digital-n-164-2024-cnsd

1.4.2. Ciberataques réplica

Son aquellos que utilizan las TIC para facilitar la comisión de delitos tradicionales. Así, su nacimiento no está supeditado a la aparición del Internet, sino que ven en las herramientas propias del ciberespacio un medio que ayuda a su comisión, a su anonimato o a su impacto: "Se trata, por tanto, de réplicas llevadas a cabo en el ciberespacio de crímenes que ya se realizaban, de otro modo, en el espacio físico. Sin embargo, los especiales caracteres de este nuevo ámbito de realización criminal que es el ciberespacio confiere a la conducta una singularidad tal, que la hacen aparecer prácticamente como una conducta nueva, hasta el punto de que lo que en el espacio territorial podía apenas tener relevancia dañina, puede adquirirla significativamente en el espacio virtual"[80].

1.4.2.1. Ciberfraudes

Ataques *online* contra usuarios (individuos o instituciones) que tienen como objetivo obtener un beneficio económico indebido en perjuicio de la víctima. Entre las modalidades más frecuentes se encuentran las estafas por medios tecnológicos o virtuales y los fraudes informáticos.

[Caso 13] Armando Vásquez Martínez y Hermes Vergara Zamora, con la asistencia de Erickson Antonio Araujo y Wilson Armas Pezo, mediante la modalidad de *pharming*, se apoderaron de 9 600 soles que Edy Quispe Gallegos mantenía en el Banco de Crédito del Perú.

La defensa del encausado Vásquez Martínez impugnó la sentencia alegando que (i) no se acreditó que realizó operaciones de transferencia o envíos de correos electrónicos, (ii) la entrega de tarjetas bancarias a su cosentenciado no configura el delito de fraude informático, (iii) no se logró identificar a la persona que infectó la máquina de la víctima, (iv) el envío de correos electrónicos fraudulentos son de procedencia americana, (v) solo se logró identificar el IP desde el cual se realizaron las tres operaciones objeto de cuestionamiento, pero no vincularlo con un lugar o persona específica y

80 Miró Llinares, *El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio*, cit., p. 68.

(vi) las contradicciones incurridas por un testigo impropio. La Corte Suprema desestimó el recurso a partir del análisis de la prueba testimonial y documental, y confirmaron la sentencia por el delito de fraude informático -previsto en el art. 8 LDI-[81].

1.4.2.2. Phishing

Tipo de ataque en el que se suplanta a una persona, una entidad o un servicio mediante algún medio de comunicación -correo electrónico, mensajes de texto, de redes sociales o, incluso, llamadas telefónicas- para obtener las credenciales (contraseñas) o información bancaria de la víctima. En algunos casos, se acompaña un enlace que redirige a una página suplantadora. Entre las modalidades más frecuentes se encuentran: *vishing* (*voice* + *phising*), *smishing* (SMS + *phishing*) y *QRshing* (QR + *phising*).

[Caso 14] El 4 de junio de 2011, a las 11:15 am, José Francisco se encontraba realizando operaciones a través de la web del banco español Ibercaja cuando la interfaz se bloqueó. De repente, empezó a recibir mensajes de texto (SMS) de su banco, supuestamente, en los que se solicitaban sus claves. Las brindó pensando que era la entidad financiera. Al comunicarse por teléfono, Ibercaja le informó que desde su cuenta se habían transferido 2 000 euros a una cuenta que la víctima desconocía. Cuatro días después, un evento similar le ocurrió a Cecilio, quien transfirió 1 900 euros a una cuenta también desconocida.

En el proceso se descubrió que la transferencia de José Francisco fue recibida en la cuenta de Tomás, la misma que estaba asociada a su número celular personal. Durante el día que recibió la transferencia, Tomás la reenvió a Rogelio. Sucedió lo mismo con el dinero de Cecilio: fue recibida por Tomás y reenviada a Rogelio. Si bien ambos alegaron ignorancia, fueron condenados por el delito continuado de estafa ya que "los acusados realizaron un acto de relevancia, dado que, con su participación, reforzaron la maquinación fraudulenta, contribuyendo al buen fin del negocio, facilitando la produc-

81 R. N. N.º 2932-2016, Lima del 12 de junio del 2017, emitida por la Primera Sala Penal Transitoria de la Corte Suprema de Justicia.

ción del resultado, por facilitar sus números de cuentas bancarias para que se realizaran en las mismas las transferencias no consentidas por sus titulares"[82].

[**Caso 15**] Investigadores de la empresa de ciberseguridad Confense detectaron un nuevo troyano de acceso remoto denominado *Poco RAT*. Este *malware* es distribuido a través de una campaña de *phishing* por correo electrónico, dirigido a empresas del sector minería, manufactura, hotelería y servicios públicos en países de habla hispana. La víctima recibe un correo de temática financiera que contiene un enlace a un archivo 7 zip alojado en Google Drive -para eludir las medidas de seguridad-. Una ataque exitoso compromete información confidencial, credenciales y expone al usuario a posibles ataques futuros de *ransomware*[83].

1.4.2.3. Pharming

Según el Glosario de Términos de Ciberseguridad, publicado por el Instituto Nacional de Ciberseguridad de España, es un "[a]taque informático que aprovecha una vulnerabilidad del *software* de los servidores DNS y que consiste en modificar o sustituir el archivo del servidor de nombres de dominio cambiando la dirección IP legítima de una entidad (comúnmente una entidad bancaria) de manera que en el momento en el que el usuario escribe el nombre de dominio de la entidad en la barra de direcciones, el navegador redirigirá automáticamente al usuario a una dirección IP donde se aloja una web falsa que suplantará la identidad legítima de la entidad, obteniéndose de forma ilícita las claves de acceso de los clientes a la entidad".

[**Caso 16**] El 24 de agosto de 2021, Nuria, administradora de la junta de propietarios de su edificio, introdujo los datos y claves de su cuenta en una página web simulada del banco Ibercaja. Esa transferencia fue recibida en la cuenta de Joaquina, quien dispuso inmediatamente de dicho dinero. Si

82 SAP 1105/2023. Sentencia N.º 203/2023 del 12 de junio de 2023, emitida por la Audiencia Provincial de Zaragoza, Sección N.º 3. Ponente: Nicolasa García Roncero.

83 Centro Nacional de Seguridad Digital. *Alerta integrada de seguridad digital N.º 162-2024*. Lima: 12 de julio de 2024, p. 7. https://www.gob.pe/institucion/pcm/informes-publicaciones/5776792-alerta-integrada-de-seguridad-digital-n-162-2024-cnsd

bien no se identificó al responsable de la creación del sitio web fraudulento, Joaquina fue condenada como *mula bancaria* al considerarse cómplice necesaria[84].

1.4.2.4. Scam

Es un tipo de estafa cometido a través de las TIC. Entre las modalidades más comunes se encuentran el empleo de campañas de correo electrónico y las páginas web falsas. Por lo general, se emplean técnicas de ingeniería social para engañar a la víctima.

[Caso 17] Bruno, Constancio, Doroteo, Victoriano, Milán y Luis Miguel, junto a otras personas no identificadas, formaron, entre el 2012 y el 2016, una agrupación dedicada a cometer estafas y defraudaciones a través de ingeniería social en España. Así, se descubrió que estaban involucrados en el envío de "cartas nigerianas", ofrecimiento de supuestos premios de lotería que requerían de un pago previo, herencias, ofertas de trabajo, usurpación de cuentas de correos electrónicos, creación de falsas páginas web de entidades financieras y de empresas, captación de víctimas para supuestas necesidades de enviar dinero al extranjero, entre otras técnicas. La organización operó en más de 35 países del mundo, hasta que el operativo policial *Galáctico* logró descubrir a algunos de sus integrantes.

En el proceso se descubrió que uno de sus miembros viajaba continuamente a Palma para abrir cuentas corriente. Este, además, administraba dos co-

84 SAP 78/2024. Sentencia N.º 35/2024 del 26 de enero de 2024, emitida por la Audiencia Provincial de Zaragoza, Sección N.º 6. Ponente: Francisco José Picazo Blasco. En el tercer considerando de la resolución se describe el *pharming* en los siguientes términos: "Los defraudadores simulan o copian una página web de un banco y en los correos anzuelo incluyen una URL en la que el cliente destinatario víctima ha de pinchar, teóricamente para acceder a la página web de su banco pero que, en realidad les dirige a la página web simulada donde el destinatario introducirá sus datos de usuario y contraseñas, valiéndose de una excusa lo más verosímil posible (actualización del sistema, verificación de datos, etc.)".

rreos electrónicos que fueron denunciados en portales *anti-scam* por estar vinculados a estafas por internet[85].

1.4.2.5. Auction fraud

Es un tipo de estafa *online* que se comete en las plataformas de subastas. Entre las modalidades más frecuentes se encuentran: venta de productos falsos, no entregar los productos después de haber recibido el pago, utilizar cuentas falsas para elevar el precio del producto o servicio ofrecido o utilizar técnicas de ingeniería social -como el *phishing*- para obtener datos personales.

[**Caso 18**] Entre el 8 y el 12 de febrero de 2004, Paulino ofreció celulares y monitores a través de la página web de subastas y comercio electrónico e-Bay. Los ofertantes, pensando que cumpliría con lo pactado, realizaron diversas transferencias por los productos subastados: (i) Pablo Jesús transfirió 161,80 euros por dos celulares; (ii) Alejandro, 304 euros por un celular; (iii) Cosme, 82 euros por un celular; (iv) Gabriel, 85 euros por un celular; (v) Marcial, 304 euros por un celular; (vi) Vicente, 318,40 euros por un monitor; y (vii) Patricio, 915 euros por tres celulares.

La misma modalidad de estafa a través de subastas de productos no entregados fue empleada por sus coacusados -todo lo cual fue corroborado en el proceso-. Paulino y sus coacusados fueron condenados por estafa en el 2015[86].

1.4.2.6. Cyberspyware

Conocido también como espionaje cibernético o ciberespionaje. Es un tipo de ataque en el que individuos, grupos, empresas, organismos gubernamentales u organizaciones terroristas usan las TIC para obtener información o

85 STS 469/2022. Sentencia N.º 42/2021 del 18 de enero del 2022, emitida por la Salade lo Civil y Penal del Tribunal Superior de Justicia de Palma de Mallorca, Sección N.º 1. Ponente: Antonio Federico Capo Delgado.

86 SAP 8452/2015. Sentencia N.º 37/2015 del 11 de junio de 2015, emitida por la Audiencia Provincial de Madrid, Sección N.º 30. Ponente: María Pilar Olivan Lacasta.

acceso no autorizado a los sistemas informáticos de la víctima. Por lo general, se utiliza *malware* que recopila información de la víctima y la envía, sin su conocimiento o consentimiento, al atacante.

[Caso 19] Según la tesis fiscal, el 17 de agosto de 2003, Cecilio, desde su domicilio ubicado en Alcalá de Henares, España, creó el virus Kelar, también llamado Raleka. Este virus infectaba a usuarios de Panda, quienes se conectaban a una página web maliciosa, descargaban un troyano que le permitía al atacante tomar el control y acceso remoto de los ordenadores. Entre el 17 y el 28 de agosto, 70 mil usuarios habrían descargado tanto el virus como el troyano.

Si bien Cecilio reconoció haber creado el virus -denominándole, programa-, para la Corte no se acreditó que se haya apoderado o utilizado datos reservados de los usuarios, sino que únicamente generó un riesgo potencial. Así, se concluye, a partir de las declaraciones brindadas por el agente de la Guardia Civil que practicó la entrada y registro del inmueble de Cecilio, un jefe de seguridad informática, un testigo y un perito, que "no hay la más mínima evidencia de que el acusado hubiera accedido, modificado o utilizado datos de carácter reservado, personal o familiar, sino únicamente una posibilidad de hacerlo, posibilidad no tipificada en nuestro ordenamiento jurídico y que, por lo tanto obliga a absolver al acusado del delito analizado"[87].

1.4.2.7. Uso de sniffers

Tipo de ataque en el que se emplean herramientas o programas para revisar el tráfico de una red y, de este modo, capturar los paquetes de información que se envían o reciben.

[Caso 20] Entre el 21 de julio de 1998 y el 3 de setiembre de 1999, Héctor trabajó como administrador de sistemas en la empresa Seric Informática. Aprovechándose de su puesto, accedió a diversos códigos fuente y base de

87 SJP 48/2014. Sentencia N.º 238/2014 del 24 de junio de 2014, emitida por el Juzgado de lo Penal de Alcalá de Henares, Sección N.º 4. Ponente: Nuria Alcalde Alcalde.

datos que incluían información de numerosos clientes, copiándolos e instalándolos en su ordenador personal.

Pese a ser desvinculado, siguió accediendo a los sistemas de la empresa empleando las claves de acceso de otro trabajador. Cuando la empresa sospechó de la actividad ilegal, instaló un *sniffer*. Este programa recogió la actividad desarrollada por una cuenta de correo con la que se conectaban otros dos, los cuales eran manejados por Héctor y su pareja sentimental. Héctor fue condenado por el descubrimiento de secretos de la empresa agraviada[88].

1.4.2.8. Ciberespionaje de empresas

Conocido también como *ciberespionaje corporativo* o *industrial*, es realizado contra empresas con la finalidad de tener una ventaja competitiva a través de la obtención de información secreta o confidencial.

[Caso 21] Red Curl -también conocido como Earth Kapre y Red Wolf- es un grupo de ciberdelincuentes de habla rusa que aprovecharon un componente legítimo de Microsoft Windows denominado *Asistente de compatibilidad de programas* para ejecutar comandos maliciosos. Así, desde el 2018, realizó ataques de ciberespionaje corporativo contra entidades ubicadas en Australia, Canadá, Alemania, Rusia, Eslovenia, Reino Unido, Ucrania y Estados Unidos.

En junio de 2023, se reveló que un banco ruso y una empresa australiana fueron atacadas por este grupo de ciberdelincuentes, quienes robaron secretos corporativos confidenciales e información de los empleados[89].

[Caso 22] El 30 de julio de 2020, el Consejo de la Unión Europea dio a conocer que, por primera vez en su historia, se impusieron sanciones en respuesta a ciberataques de gran magnitud. Así, se impusieron medidas

88 SAP 623/2003. Sentencia N.º 127/2003 del 4 de abril de 2003, emitida por la Audiencia Provincial de Tarragona, Sección N.º 2. Ponente: Xavier Nouvilas Puig.

89 Centro Nacional de Seguridad Digital. *Alerta integrada de seguridad digital N.º 64-2024*. Lima: 14 de marzo de 2024. p. 5. https://www.gob.pe/institucion/pcm/informes-publicaciones/5367163-alerta-integrada-de-seguridad-digital-n-064-2024-cnsd

restrictivas contra seis personas y tres entidades responsables de ciberataques contra la Organización para la Prohibición de las Armas Químicas y los responsables de WannaCry, NotPetya y Operation Cloud Hopper (este último es un caso de ciberespionaje que involucró, en el 2017, a una red organizada en China).

Entre las sanciones impuestas figuran la prohibición de viajar y la inmovilización de fondos. Además, las personas y entidades de la Unión Europea tienen prohibido poner fondos a disposición de los responsables. Es importante precisar que estas medidas integran un conjunto de instrumentos de ciberdiplomacia consensuados para impedir, disuadir y responder a los ataques informáticos[90].

1.4.2.9. Identity theft

Conocido como *robo* o *suplantación de identidad*. En esta tipología de ataque, el ciberdelincuente utiliza la identidad de la víctima -imagen o datos personales- para suplantarla e interactuar con determinadas personas. Esta conducta se asocia con otras modalidades delictivas como el *grooming* -el atacante utiliza la identidad de un menor de edad para relacionarse con la víctima- o estafas *online* -el atacante utiliza la identidad de algún familiar o amigo para engañar a la víctima-.

[Caso 23] El 8 de setiembre de 2022, la congresista fujimorista Tania Ramírez García[91] (@taniaramirezga2) denunció ante la Fiscalía de la Nación ser víctima de suplantación de identidad en la red social Twitter, ahora X, por la cuenta @taniaraimirez. La cuenta suplantadora utiliza la imagen de la legisladora, su nombre completo e imagen de portada, sin embargo, tiene una curiosa descripción: "*Queen Tendera. Hago Tik toks y tengo las uñas largas (Parody)*"[92]. A marzo de 2025, la cuenta verdadera tiene 18 944 seguidores

90 Consejo de la Unión Europea. "La UE impone por primera vez sanciones en respuesta a los ciberataques", 30 de julio de 2020. https://www.consilium.europa.eu/es/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/

91 Cuenta de la congresista Ramírez: https://x.com/Taniaramirezga2

92 Cuenta parodia: https://x.com/TaniaRaimirez

mientras que la otra, 13 921. Esto nos lleva a la siguiente reflexión: ¿cuál es el límite de la parodia y el humor en entornos digitales?



Imagen 4. Comparación de la cuenta original de la congresista Tania Ramírez García con la cuenta parodia o posiblemente suplantadora de identidad.

[Caso 24] El 17 de mayo de 2022, Naditza Acasiete fue condenada a 3 años y 20 días de pena privativa de libertad y al pago de 2 000 soles por reparación civil al haber creado una cuenta falsa a nombre de Carmen Rosa Herrera, en Facebook[93].

93 Ministerio Público. "Ministerio Público logró sentencia por creación de perfil falso en Facebook", 18 de mayo de 2022. https://www.gob.pe/institucion/mpfn/

El Décimo Juzgado de Investigación Preparatoria dictó sentencia de terminación anticipada tomando en consideración (1) la denuncia directa del 15 de julio de 2021, (2) los anexos de la denuncia que daban cuenta de la cuenta falsa, (3) el acta de comunicación telefónica y la conservación de datos en Facebook, (4) el acta fiscal de exportación de Facebook, (5) el acta de visualización de perfil de Facebook del 26 de julio de 2021, (6) el acta de declaración de la agraviada, (7) las dos actas de declaraciones testimoniales, (8) el acta de autorización dirigida a la empresa de telefonía, (9) el acta de declaración de la investigada, entre otros. Esta relación de elementos nos lleva a una reflexión: ¿las pruebas hubiesen justificado una condena en un eventual juicio oral?

1.4.2.10. Spoofing

Tipo de ataque que consiste en falsificar, suplantar o imitar algo o a alguien. De acuerdo con el Instituto Nacional de Ciberseguridad, "es un ciberataque en el que el ciberdelincuente se hace pasar por una fuente confiable (entidades bancarias, instituciones públicas, proveedores, clientes, compañías telefónicas, aplicaciones, etc.), para hacerse así con sus datos privados y credenciales sin que los afectados lo sepan y así poder filtrarlos, chantajearles, propagar *malware* a través de archivos adjuntos, o enlaces infectados, robar dinero, etc. [sic]".

[Caso 25] En mayo del 2021, se tomó conocimiento de una campaña de descarga de *malware* a través correos electrónicos que suplantaban a la empresa DHL. La víctima recibía un correo cuyo asunto era "FW: su confirmación / notificación de envío de DHL Express". En el correo se señalaba que la empresa intentó comunicarse sin éxito con el destinatario para que recoja un paquete enviado a su nombre. Se adjuntaba una "factura", sin embargo, el archivo era de tipo .rar, un *malware* que comprometía la seguridad del equipo infectado[94].

noticias/607633-ministerio-publico-logro-sentencia-por-creacion-de-perfil-falso-en-facebook

94 Centro Nacional de Seguridad Digital. *Alerta integrada de seguridad digital N.º 108-2021.* Lima: 6 de mayo de 2021, p. 4. https://www.gob.pe/institucion/pcm/infor-

1.4.2.11. DNS spoofing

Conocido como *suplantación de DNS* o *suplantación de nombre de dominio*. El ciberdelincuente infecta y accede al *router* de su víctima[95]. De este modo, el atacante utiliza registros de DNS alterados para redirigir el tráfico en línea a un sitio web o dominio fraudulento.

[Caso 26] En este caso, la víctima envía un requerimiento de acceso a una página web veraz, sin embargo, el servidor ha sido *envenenado*, redirigiendo al cliente a una página falsa: (1) solicitud de acceso a una página web real; (2) el atacante inyecta una entrada DNS falsa; (3) el usuario es redirigido a una página web falsa.

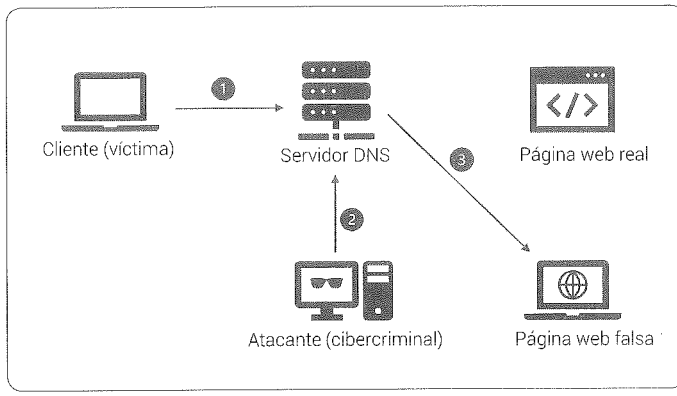


Diagrama 1. Esquema de ataque por envenenamiento de DNS. Elaboración propia

1.4.2.12. ARP spoofing

Conocido como *suplantación de ARP* o *envenenamiento de caché ARP*. El atacante envía mensajes ARP falsos a través de la Ethernet o red del área local. De este modo, se vincula la dirección MAC del atacante con la dirección IP

mes-publicaciones/1896577-alerta-integrada-de-seguridad-digital-n-108-2021-pecert

95 "*Router*. Dispositivo de red que traslada los paquetes de una red a otra. Basándose en las tablas y protocolos de enrutamiento y en el origen y destino, un *router* decide hacia dónde enviar un paquete de información. Conecta redes múltiples, tales como una red local e internet. Opera en la capa tres (nivel de red)" (Angulo Aguirre, Luis. *Hacking & cracking – Redes inalámbricas Wi-Fi*. Lima: Macro, 2018, p. 233).

de un dispositivo o servidor verdadero de la red. Según el glosario de términos de seguridad de INCIBE, "al falsear la tabla ARP de la víctima, todo lo que se envíe a un usuario, será direccionado al atacante".

[Caso 27] El ataque del hombre del medio o Man-in-the-Middle (MiTM), se caracteriza porque el ciberdelincuente envía respuestas ARP falsas a una determinada dirección IP, lo que origina que el dispositivo de la víctima llene su caché ARP con la dirección MAC del atacante, en lugar de la dirección MAC del *router* local. De este modo, la máquina afectada enviará incorrectamente el tráfico de red al atacante.

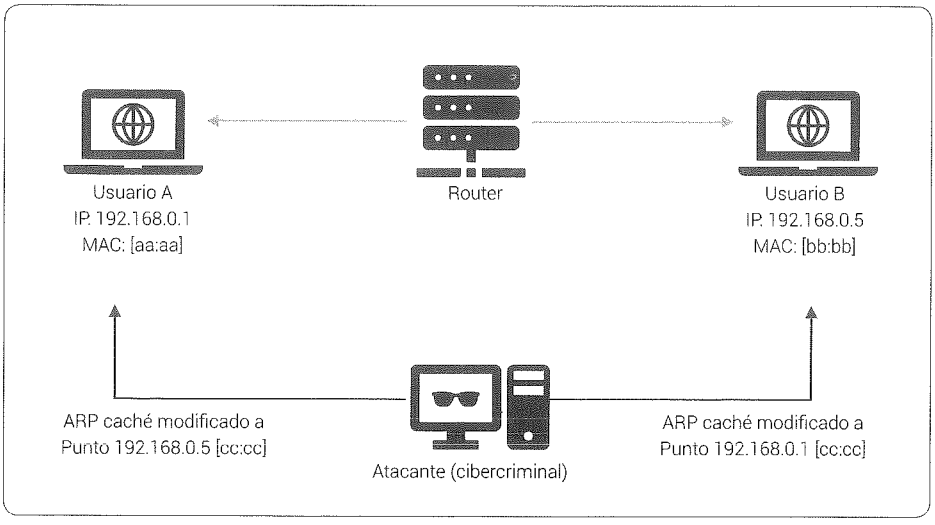


Diagrama 2. Esquema de ataque por ARP *spoofing*. Elaboración propia.

1.4.2.13. IP spoofing

Conocido como *suplantación de IP*. El ciberdelincuente oculta su identidad falsificando su dirección de IP de origen. De acuerdo con el Instituto Nacional de Ciberseguridad de España, el atacante engaña a los sistemas de seguridad de la red para ser considerado como una fuente fiable.

[Caso 28] Se acusó a Rosendo de apoderarse de los datos bancarios de la tarjeta de Laura y efectuar dos compras por un valor ascendente a 296,82

euros, el 18 de junio de 2015, desde su domicilio en Alcantarilla, Murcia. Con ese dinero se adquirió un servidor virtual (VPS), una licencia de panel Plesk edición Web Host, un hosting web modelo Business, el registro por un año del dominio www.salutechkres.com y una compra en línea en la consola de PlayStation.

El investigado manifestó que él también fue víctima de un ciberataque, ya que desconocidos habrían utilizado su IP para enmascarar su ubicación. En el proceso se aportó una pericia que concluía que "la inferencia que vincula ser usuario de un ordenador y línea telefónica no conlleva necesariamente a la conclusión de que ese usuario sea el autor de toda utilización telemática de esa infraestructura telemática [sic]". Rosendo fue absuelto, ya que la investigación no fue rigurosa y subsistía la posibilidad de que haya sido víctima de IP *spoofing*[96].

1.4.2.14. Web spoofing

Conocido como *suplantación web*. El delincuente diseña una página web idéntica o muy similar a la legítima para que la víctima interactúe con ella -por ejemplo, brindando datos personales o bancarios-. Esta técnica se suele combinar con el *typosquatting*, una modalidad de ciberocupación.

[Caso 29] El 13 de abril de 2021, Germán recibió una solicitud de actualización de información bancaria. El enlace lo redirigió a un sitio web falso que imitaba la página del Banco Santander. Se le solicitó realizar una operación de *comprobación*, motivo por el cual efectuó una transferencia de 3 500 euros. Concepción recibió el dinero e, inmediatamente, lo retiró.

Si bien Concepción alegó que cometió un error, pues pensó que se trataba de una subvención social, este argumento fue desestimado, ya que no había formulado ningún pedido de esta naturaleza y, además, incurrió en contradicciones a lo largo del proceso. Fue condenado[97].

96 SAP 636/2016. Sentencia N.º 205/2016 del 29 de junio de 2016, emitida por la Audiencia Provincial de Valladolid, Sección N.º 4. Ponente: Ángel Santiago Martínez García.

97 SAP 2160/2022. Sentencia N.º 345/2022 del 28 de setiembre de 2022, emitida por la Audiencia Provincial de Vigo, Sección N.º 5. Ponente: José Ramón Sánchez Herrero.

1.4.2.15. Ciberblanqueo de capitales

Es una modalidad de lavado de activos en el que se emplean las recursos y plataformas en línea para ocultar y transferir fondos obtenidos de actividades delictivas como, por ejemplo, criptomonedas, herramientas que permiten cifrar o encriptar datos, así como su anonimización.

[Caso 30] Los cárteles de Jalisco Nueva Generación y de Sinaloa estarían utilizando criptomonedas para dificultar el rastreo de dinero maculado o utilizarlo de manera *segura*[98]. Así, según el último reporte publicado por la DEA, los cárteles mexicanos y otras organizaciones de tráfico de drogas utilizan las criptomonedas para blanquear los ingresos ilícitos:

> Los lavadores de dinero que poseen criptomonedas recogen dinero en efectivo a granel de los traficantes de drogas y transfieren criptomonedas a los traficantes de drogas a cambio. Los traficantes de drogas pueden transferir inmediatamente la criptomoneda a sus contrapartes en México u otros países donde generalmente se revende por moneda local. La naturaleza ultracifrada de estas transacciones, y la dificultad para rastrearlas sin la "clave" del traficante, hace que sea casi imposible medir el alcance de la actividad de lavado de dinero que ocurre en el espacio de las criptomonedas.
>
> Los traficantes de drogas también lavan sus ingresos de drogas a través de empresas de intercambio de criptomonedas, que están obligadas por la ley de los Estados Unidos a monitorear a los clientes y las transacciones en busca de indicios de lavado de dinero. Los traficantes de drogas hacen depósitos estructurados de dinero en efectivo en cuentas bancarias que se utilizan para comprar criptomonedas a través de intercambios en línea. Una vez que los ingresos de la droga en efectivo se utilizan para comprar criptomonedas, la criptomoneda se puede revender rápidamente por dinero en efectivo u otro instrumento financiero a cualquier otro comprador de criptomonedas en todo el mundo[99].

98 "Bitcoin: así lo usan carteles del crimen para lavar dinero (y las autoridades para desmantelarlos)", en *France 24 Español*, 10 de diciembre de 2020. https://youtu.be/6E__nE3eSBI?si=ItojxqGeTEPYnOUR

99 Drug Enforcement Administration. *National Drug Threat Assessment 2024*, p. 48. https://www.dea.gov/sites/default/files/2024-07/2024%20NDTA-updated%207.5.2024.pdf

1.4.2.16. Ciberextorsión

Es una extorsión *online*. Tipo de ataque por el cual el delincuente exige a la víctima (empresas o individuos) el pago de un rescate a cambio de recuperar el acceso a un sistema informático, no difamarla, no divulgar contenido íntimo o confidencial, entre otros ilícitos requerimientos.

[Caso 31] El grupo ruso Qilin, mediante un ataque de *ransomware*, afectó a diversos centros de salud de Londres -entre ellos, el laboratorio de Patología Synnovis-[100]. El *malware* empleado utiliza una combinación de cifrado simétrico y asimétrico para bloquear los archivos de la víctima. Logrado el objetivo, Qilin envía una nota de rescate solicitando el pago en criptomonedas para la liberación de los sistemas. Producto de este ataque, en junio del 2024, se cancelaron 1 134 operaciones médicas. Como la víctima no pagó el rescate (50 millones de dólares), los atacantes publicaron 400 GB de datos sanitarios confidenciales en línea -nombres de pacientes, fechas de nacimiento, número de NHS y descripción de análisis de sangre-.

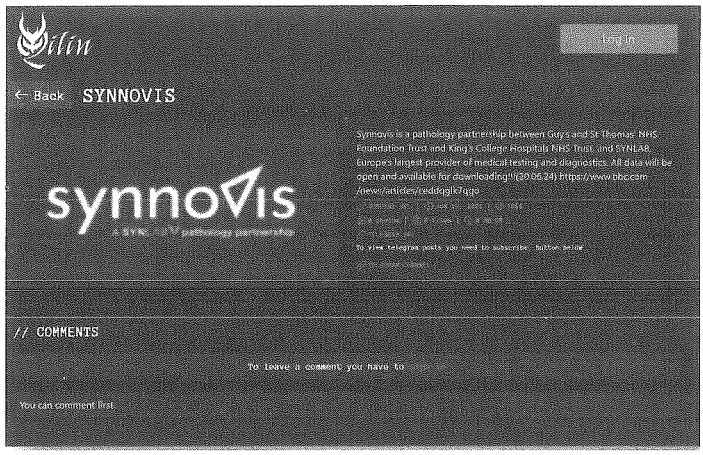


Imagen 5. Captura de pantalla de la plataforma alojada en la *dark web*. En ella, el grupo Qilin se adjudicó el ataque e informó sus alcances y demanda[101].

100 Centro Nacional de Seguridad Digital. *Alerta integrada de seguridad digital N.º 148-2024*. Lima: 26 de junio de 2024, pp. 4-5. https://www.gob.pe/institucion/pcm/informes-publicaciones/5702366-alerta-integrada-de-seguridad-digital-n-148-2024-cnsd

101 Waqas. "Qilin Ransomware leaks 400GB of NHS and Patient Data on Telegram", en *HACKread*, 21 de junio de 2024. https://hackread.com/qilin-ransomware-attack-nhs-patient-data-leak-telegram/

[**Caso 32**] En agosto de 2005, Samuel contactó a Herminia luego de apoderarse, sin su conocimiento y mediante herramientas informáticas, de archivos personales en los que la víctima aparecía desnuda o desarrollando conductas sexuales. Samuel la amenazó con difundir el contenido si no aceptaba realizar videollamadas en los que Herminia se desnudaría y realizaría actos de connotación sexual como masturbarse frente a la *webcam*. Esto ocurrió entre agosto de 2005 y mediados del 2007 y entre abril de 2009 y el 14 de diciembre del mismo año. Esta conducta se replicó con otras víctimas: Trinidad, Candia, Elsa y Graciela.

La corte resume adecuadamente el problema que existe detrás de este tipo de extorsión:

> Ante la proliferación de este tipo de casos de abusos sexuales por internet sin consentimiento de las víctimas y con el empleo de la extorsión de divulgar imágenes o videos de las víctimas se ha empezado a utilizar el término *sextorsión*, para calificar este tipo de actos de delitos de abusos sexuales cometidos por internet y con la extorsión que lleva implícita la falta de consentimiento de las víctimas. Como en este caso aquí analizado, el autor del delito de abuso sexual *online* infecta primero al ordenador de su víctima mediante un virus que le permite acceder a sus contenidos, captando imágenes y/o videos privados que pueden comprometer su intimidad si se divulgaran. Generalmente, el "modus operandi" consiste en la mecánica por la que el autor del delito envía un correo electrónico a su víctima con un enlace atractivo para ella, y al "pinchar" en el mismo se descarga el "malware" en su ordenador. Con ello, el criminal ya tiene acceso a sus contenidos y podrá descargarse archivos e imágenes o videos, que constituye luego la extorsión, lo que lleva a calificar los actos como sextorsión[102].

Al demostrarse que en el ordenador de Samuel se encontraron programas que permitían acceder, sin requerir el permiso de terceros, a archivos de forma remota, así como conocer lo que sus víctimas tecleaban (*keylogger*), y herramientas diseñadas para escanear direcciones IP, fue condenado por delitos de abuso sexual, contra la intimidad y de amenazas.

102 STS 3040/2018. Sentencia N.º 377/2018 del 23 de julio de 2018, emitida por la Sala de lo Penal de Madrid del Tribunal Supremo, Sección N.º 1. Ponente: Vicente Magro Servet.

1.4.2.17. Ciberocupación

Esta modalidad delictiva fue abordada con anterioridad como ejemplo de ataque puro, sin embargo, también puede configurar una modalidad de ciberataque réplica pues facilita la comisión de delitos tradicionales -en este caso, la estafa-.

[Caso 33] En el 2020, ciberdelincuentes lanzaron una campaña de *phishing* que combinaba el *cybersquatting*, pues adquirieron un dominio similar al del Banco de Crédito del Perú para que las víctimas no advirtieran que estaban siendo timadas[103].

Así, la URL veraz es: bcpzonasegurabeta.viabcp.com/#/iniciar-sesion. En cambio, las URL creadas para delinquir fueron:

- www[.]bcpzonasegurabeta[.]viabcp[.]live
- bcpzonasegurabeta[.]luxuryaction[.]com

1.4.2.18. Cyberstalking

Es un tipo de ciberacoso. Es el uso de las TIC para acechar o acosar a un individuo, grupo u organización. Entre las modalidades más frecuentes, tenemos las siguientes: seguimiento de la actividad en línea, enviar amenazas de muerte o similares consecuencias a través de mensajes, correos o publicaciones en redes sociales, *doxing*, envío repetido y constante de mensajes a la víctima sin su consentimiento.

[Caso 34] Hialmar Laynes Sánchez, de 54 años, fue denunciado públicamente por acosar sistemáticamente a un grupo de periodistas: Trilce Reyes, Ximena Carrasco, María Fernanda Montenegro y Manuela Camacho[104].

103 Centro Nacional de Seguridad Digital. *Alerta integrada de seguridad digital N.º 11-2020*. Lima: 15 de abril del 2020, p. 8. https://www.gob.pe/institucion/pcm/informes-publicaciones/544930-alerta-integrada-de-seguridad-digital-n-011-2020-pecert

104 "Manuela Camacho rompe en llanto al saber que Poder Judicial ordenó captura inmediata a su acosador", en *Infobae*, 16 de agosto de 2024. https://www.infobae.com/peru/2024/08/16/manuela-camacho-y-su-emotiva-reaccion-luego-de-que-poder-judicial-ordeno-captura-inmediata-a-su-acosador/; "La pesadilla del acosador que sigue

El 11 de junio de 2023, esta última lo denunció y solicitó medidas de protección a su favor. El 29 de julio de 2024, Laynes las incumplió y fue detenido. El 2 de agosto fue sentenciado por desobediencia y resistencia a la autoridad, en primera instancia. Dos semanas después, gracias a la fiscalización social y mediática -pues, el condenado seguía acosando a sus víctimas e, incluso, a la juez que dictó el pronunciamiento-, el Poder Judicial lo condenó a cinco años de pena efectiva -fecha desde que se encuentra prófugo-[105].

1.4.2.19. Cyberbullying

Es un tipo de ciberacoso. Este término se emplea principalmente cuando el acoso se produce y se dirige por y contra menores de edad (niñas, niños y adolescentes), especialmente en la escuela.

[Caso 35] René, de 13 años, fue víctima de *cyberbullying* y agresiones físicas impartidas por Adolfo, su compañero de su escuela. La madre de la víctima demandó a los padres del agresor, atribuyéndoles responsabilidad extracontractual, pues (1) su hijo le propinó un puñetazo a René el 17 de octubre de 2019 frente a sus compañeros y (2) lo amenazaba e insultaba por redes sociales. Sobre este último extremo, la Corte de Apelaciones refiere lo siguiente: "Además de ellos, están acreditados los insultos y amenazas, a través de redes sociales, que se vertían contra René. En el recurso se defiende que de las capturas de pantalla que se aportan con la demanda, solo una de ellas corresponde a su hijo Adolfo, en referencia a la última de ellas en las que se dice "no pegues a René que quiero ver otra película nueva de los pitufos". Si bien esto es cierto, lo que evidencian estas capturas es que la agresión por parte de Adolfo dio lugar a nuevas mofas y mensajes des-

libre: Hialmar Laynes enviaba hasta 80 mensajes al día a periodistas", en *El Comercio*, Lima, 22 de agosto de 2024. https://elcomercio.pe/lima/la-pesadilla-del-acosador-que-sigue-libre-hialmar-laynes-enviaba-hasta-80-mensajes-al-dia-a-periodistas-manuela-camacho-noticia/

105 "Poder Judicial ordena inmediata captura de sujeto que acosa a Manuela Camacho", en *La República*, 17 de agosto de 2024. https://larepublica.pe/sociedad/2024/08/16/caso-manuela-camacho-pj-dispone-inmediata-captura-e-internamiento-de-acosador-de-periodista-1094976

pectivos contra René por parte de sus compañeros, siendo demostrativos de la situación de acoso que estaba padeciendo René en ese momento y de la que Adolfo tenía un papel preponderante, como se demuestra con su agresión física y las manifestaciones de René en el juicio, en el sentido de que era el cabecilla"[106].

En apelación, se confirmó la sentencia, pero redujo el monto de la reparación civil de 4 000 a 3 000 euros.

1.4.2.20. Online harassment

Es una categoría genérica y mucho más amplia que engloba tanto al *cyberstalking* como al *cyberbulling*. En este sentido, es cualquier comportamiento en línea, no necesariamente delictivo, que busca incomodar a la víctima a través de las TIC.

[Caso 36] Luego de que la relación de Florencio y María llegara a su fin, el primero intentó imponer su presencia y perturbar la tranquilidad de su expareja. Así, entre el 3 y el 6 de octubre de 2019, envió decenas de mensajes y notas de voz vía WhatsApp. Entre estos desafortunadamente destacan los siguientes: "Donde te vea con el pibe te voy a reventar la boca [...] cuando te pillen las dos mujeres que van por ti vas a flipar hija de la gran p...", "Te voy a buscar en el fin del mundo", "Ahora sí vas a saber quién soy yo y me conoces un poco. Pero tú no te escapas [...]", "Estás más muerta que viva", "Te voy a amargar la vida y la relación". Florencio fue condenado y todo recurso impugnatorio, en última instancia, desestimado[107].

106 SAP 7446/2024. Sentencia N.º 288/2024 del 17 de mayo de 2024, emitida por la Audiencia Provincial de Madrid, Sección N.º 9. Ponente: Juana de la Cruz Serrano Gonzáles.

107 STS 2897/2024. Sentencia N.º 476/2024 del 22 de mayo de 2024, emitida por la Sala de lo Penal del Tribunal Supremo, Sede Madrid. Ponente: Manuel Marchena Gómez.

1.4.2.21. Sexting

No es un delito. Consiste en el envío consentido de contenido sexual o erótico por medio de las TIC. Por lo general, se envían imágenes o videos, pero también incluyen mensajes y audios (notas de voz).

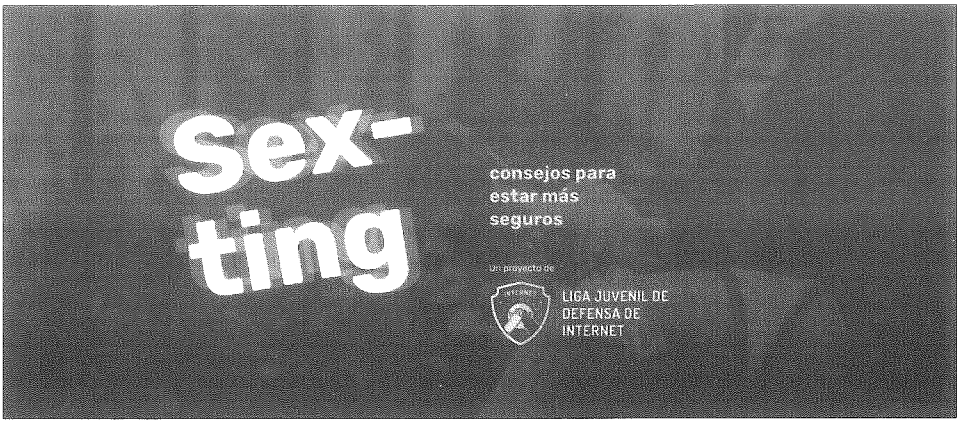


Imagen 6. En Perú, Hiperderecho y la Liga Juvenil de Defensa de Internet impulsó un proyecto muy interesante sobre el *sexting* y las medidas de seguridad que deberían adoptarse[108].

[**Caso 37**] Daniel mantuvo una relación sentimental con María Inés, con quien tuvo una hija. Por diversos problemas, entre ellos, la adicción del acusado, la relación concluyó entre marzo y junio de 2022. El 28 de julio de ese año, dado que no se le permitió ver a su hija, Daniel llamó 71 veces a María Inés, a quien insultó y amenazó con *quemarla viva*. Además, sin su consentimiento ni conocimiento, difundió en Instagram y Facebook fotografías íntimas de contenido sexual que María Inés le había enviado al inicio de la relación. Las fotos también fueron compartidas en el estado de WhatsApp de Daniel -quien, a modo de defensa, alegó que consumió abundante alcohol y fumó cocaína antes de hacerlo-.

Si bien el *sexting* no es delito, la difusión no autorizada de imágenes de contenido sexual sí lo es. En este caso, la justicia española lo subsumió bajo la figura de descubrimiento y revelación de secretos. Daniel fue sentenciado[109].

108 Ver: https://hiperderecho.org/sexting/

109 SAP 314/2024. Sentencia N.º 89/2024 del 22 de marzo de 2024, emitida por la Audiencia Provincial de Ciudad Real, Sección N.º 2. Ponente: María Almudena Buzón Cervantes.

1.4.2.22. Extorsión con imágenes de sexting

Tipo de extorsión en la cual el agresor amenaza a la víctima con difundir sus conversaciones, imágenes o videos obtenidos mediante la práctica de *sexting* si no realiza alguna acción a su favor. Por lo general, el extorsionador solicita el envío de más fotos o videos de la víctima o que esta acceda a tener relaciones sexuales.

[Caso 38] En Nueva Gales, un menor de edad fue víctima de sextorsión, pues fue amenazado con la divulgación de fotos íntimas suyas si es que no pagaba 500 dólares australianos -monto que equivale a 330 dólares americanos-. El escolar no pudo pagar y, orillado por el temor y vergüenza de que sus fotos llegasen a su familia y amigos, a fines de diciembre del 2023, se suicidó.

La policía australiana logró identificar a los ciberdelincuentes: dos hombres jóvenes que vivían en Nigeria. Al ser detenidos, en sus teléfonos se encontraron pruebas que los vincularon a más sextorsiones y víctimas[110].

1.4.2.23. Online grooming

Conocido como *grooming virtual* o *proposiciones a niños, niñas y adolescentes con fines sexuales*. El ciberdelincuente contacta a través de las TIC a un menor de edad con la finalidad de proponerle llevar a cabo un acto sexual o solicitarle material de contenido sexual.

[Caso 39] El 12 de noviembre de 2016, Mauricio contactó a Montserrat, de 12 años, a través de Instagram, sin conocerla previamente y sin preguntar cuántos años tenía. En los meses siguientes, comunicándose por Facebook y WhatsApp, averiguó su edad e inició el intercambio de mensajes de contenido sexual, proponiéndole tener encuentros sexuales.

Poco a poco se ganó su confianza, llegando a conocer que Montserrat era consumidora habitual de marihuana. Por ello, le ofreció llevar una bolsa de dicha sustancia equivalente a 100 euros. Finalmente, Mauricio la conven-

110 "Sextorstion case: Two arrested in Nigeria afeter Australia boy's suicide", en *BBC*, 8 de abril de 2024. https://www.bbc.com/news/world-australia-68720247

ció de encontrarse con él en tres ocasiones: **(i)** en junio del 2017, la besó e intentó tocarle sus genitales; **(ii)** poco después, tras ofrecerle marihuana, mantuvieron relaciones sexuales; **(iii)** en el último encuentro, Montserrat acudió con su hermano y una amiga para evitar que se produjera un nuevo encuentro sexual.

Si bien la defensa cuestionó la autenticidad de los mensajes enviados por Instagram, ya que se les impidió participar en el volcado de la información y la Corte reconoció que se encontraba frente a una prueba irregular, lo cierto es que el resto de medios de prueba subsistieron y permitieron condenar a Mauricio[111].

1.4.2.24. Ciberespionaje terrorista

Tipo de ciberespionaje realizado por organizaciones terroristas.

[Caso 40] Si bien el siguiente caso no ejemplifica el ciberespionaje terrorista, sí permite analizar el riesgo de ataques de naturaleza similar. El 19 de setiembre de 2022, un grupo de ciberdelincuentes denominado *Guacamaya Roja* publicó un comunicado en el que se señala que hackearon los sistemas militares y policiales de México, Perú, El Salvador, Chile y Colombia.

Los atacantes señalaron que esta acción formó parte de una operación mayor llamada *Fuerzas Represivas* y que sus objetivos fueron el Estado Mayor Conjunto de las Fuerzas Armadas de Chile, la Secretaría de la Defensa Nacional de México, el Comando General de las Fuerzas Militares de Colombia, la Fuerza Armada y la Policía Nacional de El Salvador, el Ejército del Perú y el Comando Conjunto de las Fuerzas Armadas del Perú.

En el caso peruano, se afirma que los cibercriminales poseerían 35 GB de información del dominio @ccffa.mil.pe y 70 GB del dominio @ejercito.mil.pe. El riesgo sería latente pues, de ser cierto, podrían exfiltrar datos confidenciales[112].

111 STSJ 1673/2023. Sentencia N.º 00062/2023 del 14 de diciembre de 2023, emitida por el Tribunal Superior de Justicia de lo Civil y Penal de Palma de Mallorca, Sección N.º 1. Ponente: Diego Jesús Gómez-Reino Delgado.

112 Centro Nacional de Seguridad Digital. *Alerta integrada de seguridad digital N.º 260-2022*. Lima: 23 de setiembre de 2022, pp. 11-12. https://www.gob.pe/institu-

1.4.3. Ciberataques de contenido

Es un tipo específico de ciberataques réplica, en el que el objeto central del injusto gira alrededor del contenido que se comunica o transmite a través de internet: "Hay que tener en cuenta además que, frente al resto de medios de comunicación, Internet funciona simultáneamente como un medio de edición y comunicación [...], donde un usuario puede pasar de ser receptor a ser comunicador y productor de contenidos [...] la ilegalidad deviene, no del medio utilizado, sino del contenido distribuido por Internet, y a las que, pese a afectar bienes jurídicos muy diferentes entre sí, les une todo un conjunto de problemáticas penales relacionadas con la distribución de contenidos: especialmente la atribución de la responsabilidad en cascada o a varios sujetos distintos (entre ellos los prestadores de servicio), o la tensión entre la eficacia en la persecución de estos contenidos con los derechos fundamentales, en general, y la libertad de expresión en particular; equilibrio que, como señaló Morón Lerma, si ya es difícil lograr en la realidad analógica, resulta aún más complejo en el ciberespacio [...]"[113].

1.4.3.1. Distribución de pornografía infantil en internet

Conocido también como *distribución de material de abuso sexual de menores en línea*. Se utilizan las TIC para producir, ofrecer, difundir, transmitir, adquirir o poseer fotografías o videos de menores de edad adoptando comportamientos sexuales explícitos. En algunos estados, también comprende la difusión de imágenes (fotos o videos) de representaciones gráficas de menores de edad o de mayores de edad simulando ser menores adoptando comportamientos sexuales.

[Caso 41] El 10 de setiembre de 2018, la Unidad Central Operativa de Policía Judicial de la Guardia Civil de España recibió una comunicación de la Homeland Security Investigations (HSI), agencia dependiente del Departamento de Seguridad Nacional de Estados Unidos. Así, se informó de la existencia de un portal alojado en la *Dark Net*, empleado para ver,

cion/pcm/informes-publicaciones/3522084-alerta-integrada-de-seguridad-digital-n-260-2022-cnsd

113 Miró Llinares, *El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio*, cit., pp. 100 y s.

descargar y distribuir material de abuso sexual infantil a través del pago de *bitcoins* o subida de archivos.

Se comprobó que Hipólito era un usuario de esta ilícita plataforma y que realizó cuatro compras: (i) 17 de abril de 2016 a las 07:34, por 51,16 euros; (ii) 10 de junio de 2016 a las 09:02, por 73,85 euros; (iii) 11 de junio de 2016 a las 07:13, por 64,33 euros; y, (iv) 16 de julio de 2016 a las 08:29, por 24,94 euros.

El 26 de marzo de 2019 se ordenó judicialmente la entrada y registro del investigado, encontrándose un ordenador, cinco discos duros, un mando con cámara oculta de memoria de almacenamiento integrada y numerosas tarjetas de memoria -en las que se localizaron miles de archivos de abuso sexual de menores de edad-. Además, se hallaron páginas web guardadas en la red TOR como favoritas de contenido sexual ilícito, *software* de tipo P2P uTorrent, un video en el que se aprecia a la sobrina del investigado, de 13 a 14 años, cambiándose, entre otros archivos ilícitos. Hipólito fue condenado por el delito de distribución y posesión de pornografía infantil[114].

1.4.3.2. Ciberpiratería intelectual

Tipo de ataque en el que se utilizan las TIC para obtener contenido protegido, republicarlo y redistribuirlo. De acuerdo a la INTERPOL, "[l]a piratería digital consiste en la copia o distribución ilegal a través de Internet de material sujeto a derechos de autor, lo que tiene efectos perniciosos para las industrias de la creación, como el cine, la televisión, la edición, la música y el juego".

[Caso 42] Entre el 2016 y el 2018, la Liga Nacional de Fútbol Profesional de España era la única cesionaria de las facultades de comercialización conjunta de los derechos audiovisuales del Campeonato Nacional de La Liga Primera y Segunda División y la Copa del Rey, con excepción de la final. La transmisión de los partidos se realizaba mediante un servicio de pago y acceso adicional a través de la codificación de la señal audiovisual.

114 SAP 2072/2021. Sentencia N.º 189/2021 del 12 de mayo de 2021, emitida por la Audiencia Provincial de Málaga, Sección N.º 3. Ponente: Juan Carlos Hernández Oliveros.

Se descubrió que Francisco era el administrador de www.verdirectotv.com, de www.verdirectotv.net y de rincondepensartv.com, plataformas en línea que alojaban canales que retransmitían los partidos sin contar con autorización de las plataformas ni de La Liga. De este modo, sin contar con autorización, entre enero del 2016 y julio del 2018, se retransmitían los partidos en las plataformas denominadas Movistar Partidazo, LaLiga 1/2/3, Multiliga y Canal +HD Liga. Además, se comprobó que bajo su administración también estaban los canales *online* Bein Sport LaLiga, Bein Sport España, Col TV y Movistar Fútbol.

El 4 de julio de 2018, se realizó la entrada y registro en el domicilio del acusado, en la localidad de Burjassot, incautando tres ordenadores con sus respectivos discos duros. Dos semanas después, el juzgado ordenó el bloqueo de las páginas investigadas. Francisco fue condenado como autor del delito contra la propiedad intelectual, en concurso con el delito contra el mercado y los consumidores, debiendo indemnizar a La Liga Nacional de Fútbol Profesional con 46 866,79 euros como monto de reparación civil[115].

1.4.3.3. Online hate speech

Conocido también como *discurso de odio en línea*. Se utilizan las TIC para difundir mensajes de odio contra personas o grupos de personas por su raza, religión, orientación religiosa o política, género, condición social o económica, etc.

[Caso 43] En enero del 2017, Aureliano, Camila, Angustia, Carlota, Apolonia, Alberto, Ascensión, Bartolomé, Benigno y Cándido integraban diversos grupos de Facebook y utilizaban esta red social para proyectar comentarios inductores al odio, desprecio y discriminación contra menores de edad por razón de su origen -nativos de Magreb o África subsahariana- y situación familiar -ingresaron solos y de forma irregular a territorio español-. En un grupo de Facebook que reunía a más de 14 mil miembros, compartieron los siguientes mensajes, entre otros:

115 SJP 31/2022. Sentencia N.º 499/2022 del 23 de diciembre de 2022, emitida por el Juzgado de lo Penal de Valencia, Sección N.º 6. Ponente: Begoña Estañ Capell.

Alberto comentó una foto compartida de un niño con puntos de sutura ante la agresión perpetrada con una botella por un *mena* -nombre con el que identifican al colectivo Menores No Acompañados-: "Eso se solucionaba dando un día de ciudad sin ley. Cómo ya la es a diario para esta bazofia. Yo le daba un día de vacaciones a la justicia y dejaba al pueblo actuar libremente y sin consecuencias [...]". Camila agregó el siguiente comentario: "Qué más da saber en qué barrio ha pasado si están por todos los rincones como RATAS, sí he dicho RATAS. Nos roban, pegan, destrozan lo que pillan, malgastamos el dinero en ellos y su bienestar ¿para qué? Uff que dios nos coja confesados!". Carlota, en la misma línea, indicó: "Tenemos que organizarnos y hacer patrullas por barrios. Ya lo hicimos una vez y limpiar las calles de esta gentuza. Solo entienden la ley del estacazo".

Al analizar los comentarios posteados, la Corte concluyó que no queda duda que se están refiriendo al colectivo *Menas*. Además, contrario a lo que sostiene la defensa, no se tratan de expresiones irreflexivas, espontáneas o incontroladas, sino de "un amplio discurso que fue fruto de una cierta maduración y que, además, el medio elegido, una red social, entraña la conciencia de hacerlo a través de un medio idóneo para que su mensaje alcance una mayor difusión, al menos en el ámbito territorial indicado" -esto es, una ciudad autónoma de apenas 13 kilómetros cuadrados de extensión territorial y de 85 mil habitantes-. Los acusados fueron sentenciados por el delito de odio[116].

1.4.3.4. Ciberterrorismo

Conocido también como *terrorismo cibernético*. Modalidad de terrorismo que tiene por finalidad dañar las TIC de la víctima (una forma de terrorismo ciberdependiente) o utilizar las TIC para facilitar la comisión de delitos vinculados al terrorismo (una forma de terrorismo cibernético), por ejemplo, para promover, apoyar, facilitar, o participar en actos terroristas.

[Caso 44] Braulio, entre el 2020 y el 17 de junio de 2023 -fecha en la que fue detenido- evolucionó en un proceso de radicalización yihadista,

116 SAN 1712/2024. Sentencia N.º 39/2023 del 6 de setiembre del 2023, emitida por la Audiencia Provincial de Melilla, Sección N.º 7. Ponente: Aaron Andueza Jiménez.

pues empleaba las redes sociales para difundir el contenido a terceros y, de este modo, captar nuevos adeptos. De esta manera, mantuvo contacto con personas que se encontraban en Siria con la intención de unirse a la organización terrorista, llegando a realizar el juramento de lealtad o Bayal a la organización *Estado Islámico-DAESH* (ISIS, por su acrónimo en inglés) y a su califa.

En la investigación se acreditó que Braulio contaba con más de 30 cuentas y perfiles en Facebook, Instagram, Youtube y Twitter, así como servicios de mensajería instantánea como WhatsApp y Telegram. Así, el adoctrinamiento -específicamente de mujeres por parte de Braulio- transitó por tres fases: (1) Barrido masivo a través de cualquier red social para obtener contacto y conexión con mujeres de cualquier parte del mundo; (2) identificar los perfiles más idóneos "y permeables a los postulados que el investigado había asumido y adherido a su ideario"; y, finalmente, (3) conversar y acercarse a las elegidas a través de Telegram -al considerarlo como un sitio seguro-.

En la investigación, se autorizó judicialmente el empleo de un agente encubierto informático, quien logró establecer contacto a través de Facebook y, luego, por WhatsApp con el investigado. Finalmente, Braulio fue condenado por el delito de autoadoctrinamiento terrorista[117].

[Caso 45] Imanol e Isaac, ambos originarios de Pakistán, a través de Facebook, Instagram y TikTok alababan y glorificaban los ataques cometidos por los seguidores del predicador fundamentalista Landelino, del partido radical Tehreek-e-Labbaik Pakistán. Así, a través de sus redes hacían llamamientos a decapitar a quienes blasfemen contra el profeta Marcial.

Entre el contenido difundido, se encuentran alabanzas hacia Plácido, autor del asesinato de dos trabajadores de la revista Charlie Hebdo. En la misma línea, se acreditó que el 26 de setiembre de 2020, Isaac compartió una composición de cinco videos referidos al mismo atentado con la siguiente descripción: "Un joven que pertenece a Pakistán intentó entrar en la oficina

117 SAN 1712/2024. Sentencia N.º 7/2024 del 5 de abril de 2024, emitida por la Sala Penal de la Audiencia Nacional de Madrid, Sección N.º 3. Ponente: Ana María Rubio Encinas.

de un periódico francés con una daga y quería matar al dueño del periódico Charlie Hebdo. Bendito valiente". En los meses siguientes, los acusados también compartieron alabanzas a favor de Ángel Daniel -ciudadano musulmán que degolló a un profesor de un colegio en París que mostró imágenes de Mahoma-, entre muchos otros. Tanto Imanol como Isaac fueron condenados por el delito de enaltecimiento terrorista[118].

1.5. CONCLUSIONES DEL CAPÍTULO

- La tecnología se ha integrado de forma natural en la vida cotidiana, afectando cómo nos comunicamos, trabajamos y consumimos información. Así, a medida que la Internet ha evolucionado desde sus orígenes hasta la actual *sociedad de la información*, se ha convertido en un espacio de oportunidades, pero también de riesgos y desafíos.
- Internet pasó de ser una red militar restringida a convertirse en una infraestructura global fundamental para la economía, la educación y el entretenimiento. Las TIC han permitido la globalización del conocimiento y la conectividad instantánea, pero las desigualdades en acceso y seguridad se encuentran latentes.
- Las TIC han beneficiado diversos sectores. A nivel industrial, impulsan la innovación, automatización y nuevos modelos de negocio. En el ámbito social, facilitan la interacción y el acceso a información, aunque generan desafíos en privacidad y protección de datos. En la educación, las TIC han revolucionado la enseñanza, aunque persisten brechas digitales y desafíos en la capacitación docente. En el plano judicial, han agilizado los procesos legales, permitiendo audiencias virtuales y, de este modo, la optimización de recursos.
- Así como las TIC generaron beneficios, también impactaron en ámbitos negativos. El ciberespacio ha facilitado la aparición de de-

118 SAN 48/2024. Sentencia N.º 1/2024 del 9 de enero del 2024, emitida por la Sala de lo Penal de la Audiencia Nacional de Madrid, Sección N.º 1. Ponente: Adoración María Riera Ocariz.

litos informáticos y la evolución o facilitación de ilícitos tradicionales. La ciberdelincuencia se manifiesta en diversas formas, desde ataques contra la seguridad informática hasta fraudes, suplantaciones de identidad y ataques contra la libertad e indemnidad sexual de menores de edad. Lamentablemente, el anonimato y la dificultad de rastreo en internet han permitido que los ciberdelincuentes gocen de cierta impunidad.

- Existen esfuerzos legislativos locales para enfrentar este nuevo fenómeno delictivo, como la Ley de Delitos Informáticos, en Perú, e instrumentos internacionales como el Convenio de Budapest o la Convención de las Naciones Unidas contra la ciberdelincuencia.
- La seguridad informática, objeto de estudio central de este libro, debe ser una prioridad para gobiernos, empresas y ciudadanos, promoviendo buenas prácticas y mecanismos de protección.

CAPÍTULO 2

LA LUCHA INTERNACIONAL CONTRA LA CIBERCRIMINALIDAD



* La ilustración de la página anterior corresponde a una adaptación de *La Paz de Münster*, de Gerard ter Borch (1648). Para su elaboración, se empleó una de las herramientas de generación de imágenes de la empresa OpenAI.

CAPÍTULO 2

LA LUCHA INTERNACIONAL CONTRA LA CIBERCRIMINALIDAD

Sumario: 2.1. Introducción. 2.2. Estudios y esfuerzos iniciales. 2.3. Estados pioneros que incorporaron los delitos informáticos en la legislación local. 2.4. Sistema europeo. 2.5. Sistema Interamericano. 2.6. Sistema de Naciones Unidas. 2.7. Conclusiones del capítulo.

> Las tecnologías han llegado tan lejos seduciéndonos con las palabras que incluso han hecho suyo el lenguaje de la naturaleza. Antes una manzana (*apple*) era algo cuya dulzura podíamos saborear, igual que podíamos escuchar el piar (*tweet*) de los pájaros al alba, o podíamos caminar con los pies metidos en la corriente (*stream*) de un arroyo y distinguir formas en las *nubes* al pasar. Ahora esas palabras se utilizan sobre todo para describir cosas que son lo contrario de la naturaleza.
>
> A quienes nos dedicamos a pensar y escribir nos corresponde desafiar todas esas sandeces corporativas y recuperar el lenguaje transparente. Llamar a las cosas por su nombre es un buen primer paso para entender mejor nuestros tiempos y luchar por un mundo mejor. Tenemos que construir nuestros propios relatos y usar las palabras que las tecnologías intentan camuflar o evitar. Tenemos que reivindicar el poder de decidir qué es conocimiento y qué no. Hablemos sobre lo que las tecnologías no quieren que hablemos [...].
>
> Carissa Véliz[119]

119 Véliz, Carissa. *Privacidad es poder. Datos, vigilancia y libertad en la era digital.* 4.ª reimpresión. Barcelona: Penguin Random House, 2023, p. 79.

2.1. INTRODUCCIÓN

Viajemos en el tiempo y transportémonos a tres momentos históricos.

[Caso 46] *Junio de 1903*[120]. En el auditorio de la Real Institución de Gran Bretaña, Londres, se encuentra el ingeniero eléctrico John Ambrose Fleming. A 500 kilómetros, en Cornualles, extremo sur de la isla británica, se ubica el inventor e ingeniero Guillermo Marconi. Una gran audiencia espera la hazaña prometida: Enviarán un mensaje entre estos dos lugares y sintonizarán sus instrumentos para que ningún otro interfiera el envío.

El público se retira maravillado, pues fueron testigos de la transmisión de un mensaje sin conexiones físicas. Sin embargo, como no sabían descifrar código morse, no advirtieron que el mensaje decía: "Ratas [...] Un joven italiano engañó al público con gran habilidad"[121]. La comunicación había sido interceptada. Cuatro días después, el autor dio a conocer su identidad mediante una carta dirigida al diario *The Times*. Se trataba del mago Nevil Maskelyne, quien indicó que se trató de una demostración que reveló los problemas de seguridad del sistema. Nos encontramos frente el primer *ataque informático*.

[Caso 47] *Francia en la Segunda Guerra Mundial*[122]. En 1940, la Alemania nazi requería realizar un censo nacional para conocer cuántos judíos vivían en la Francia ocupada -así como sus características y condiciones específicas-. Esta labor no se pudo llevar a cabo porque el material necesario para operar las máquinas tabuladoras Hollerit era muy escaso y, en consecuencia, costoso.

El 19 de diciembre de 1941, el director de la Comisión General para Asuntos Judíos, Xavier Vallat, reconoció que necesitaba ayuda para procesar la información que los nazis requerían, encargando esta labor a René Carmi-

120 Sobre este episodio histórico, ver: Raboy, Marc. *Marconi: The man who networked the world*. New York: Oxford University Press, 2016.

121 Raboy, *Marconi: The man who networked the world*, cit., p. 223.

122 Sobre este episodio histórico, ver: Black, Edwin. *IBM and the Holocaust. The strategic alliance between Nazi Germany and America's most powerful corporation*. Edición expandida. Washington: Dialog Press, 2012. [e-Book].

lle, contralor general del ejército francés. Carmille tuvo acceso a 120 000 tarjetas que contenían valiosa información, pero sus resultados no eran los esperados. Algunos años después, se descubrió que era un agente encubierto y que había alterado el sistema informático para ocultar datos sensibles y proteger al pueblo judío residente en Francia:

> Carmille había engañado a los nazis. De hecho, había estado trabajando con la contrainteligencia francesa desde 1911. Durante los peores días de Vichy, Carmille siempre fue considerado uno de los operativos de más alto rango de la resistencia francesa, miembro de la llamada "Red Marco Polo" de saboteadores y espías. La operación de Carmille había generado unos 20 000 pases de identidad falsos. Además, había estado trabajando durante meses en una base de datos de 800 000 exsoldados en Francia que podrían ser movilizados instantáneamente en unidades bien planificadas para luchar por la liberación. Según su plan, 300 000 hombres estarían listos para actuar. Tenía sus nombres, direcciones, sus especialidades militares y todas sus habilidades ocupacionales. Sabía cuáles eran trabajadores de metal especializados en barras de cortina y cuáles eran tropas preparadas para el combate
>
> En cuanto a la columna 11 que preguntaba por la identidad judía, los agujeros nunca se perforaron, las respuestas nunca se tabularon. Más de 100 000 tarjetas de judíos que estaban en su oficina nunca fueron entregadas. Él frustró toda la operación.[123].

Carmille falleció el 25 de enero de 1945, pero su labor permitió minimizar el número de judíos deportados, en Francia, a los campos de concentración. Es considerado el primer *hacker* de la historia.

[Caso 48] Estados Unidos, 1971[124]. El ingeniero de sistemas Bob Thomas creó y esparció en ARPANET el gusano Creeper o Enredadera -considerado como el primer virus informático de la historia- que, al infectar una

123 Black, *IBM and the Holocaust. The strategic alliance between Nazi Germany and America's most powerful corporation*, cit., p. 329.

124 Sobre este episodio histórico, ver: Marion, Nancy E. y Jason Twede. *Cybercrime. An Encyclopedia of Digital Crime*. California: ABC-Clio, 2020. [Kindle]

máquina, reproducía el siguiente mensaje: "Soy la enredadera: Atrápame si puedes". Thomas creó el programa sin ningún tipo de intención maliciosa, pero algunos reportaron que el gusano se replicaba con tanta frecuencia que ciertos programas no podían ejecutarse. De hecho, el diseñador tomó el nombre de un personaje de la serie de dibujos *Scooby Doo, ¿dónde estás tú?* Ese mismo año, el programador informático Ray Tomlinson creó el programa Reaper o Podadora, que eliminó el virus de las máquinas afectadas. El primer antivirus fue creado.

A lo largo de la historia de la informática, hemos sido testigos de una variedad de acontecimientos, algunos lúdicos que nos han hecho disfrutar de la creatividad tecnológica, y otros heroicos, donde innovadores han superado grandes desafíos para ayudar a la humanidad. Sin embargo, no todo ha sido positivo. También hemos presenciado ataques devastadores, como ciberataques que han puesto en riesgo la economía global y la seguridad personal, que nos recuerdan los peligros inherentes al mundo digital en el que vivimos. En las líneas siguientes, analizaremos los esfuerzos internacionales para luchar contra este novedoso fenómeno delictivo.

2.2. ESTUDIOS Y ESFUERZOS INICIALES[125]

Desde la academia, es importante recordar y reconocer a quien es considerado como el fundador y padre de la investigación de la delincuencia informática: Donn B. Parker, quien participó en la investigación más exhaustiva realizada sobre este fenómeno en 1970, documentando más de 1000 casos reportados en el mundo. Además de ser Consultor Senior de Seguridad Informática en el Instituto de Investigación de Stanford, fue el autor de primer manual federal básico para la aplicación de la ley en Estados Unidos, titulado *Computer Crime: Criminal Justice Resource Manual on Computer Crime*, publicado en 1979.

125 El recuento de los autores, sus trayectorias y obras ha sido tomado de: SCHJOLBERG, *The history of cybercrime*, cit., pp. 19 y s.

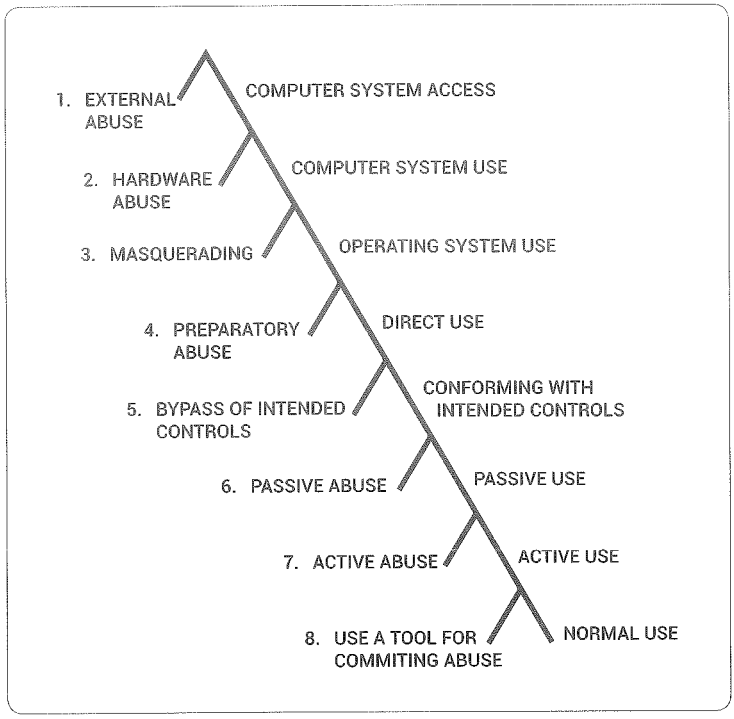


Diagrama 3. Tipos de delitos informáticos (*computer abuse*). Elaborado por Donn B. Parker[126].

Este manual se estructuró en siete secciones -las cuales detallo en su idioma original- que permitieron entender e investigar adecuadamente esta nueva modalidad delictiva: (1) Classifying the Crime, (2) Computer Abuse Methods and Detection, (3) Experts and Suspects, (4) The Computer Crime Environment, (5) Computer Crime Prosecution, (6) Computer Crime Law y (7) Overview of Computer and Communications Technology[127].

126 Parker, *Computer Crime: Criminal Justice Resource Manual*, cit., p. 4.

127 El manual, además, de incluir un glosario de términos, recoge nueve anexos muy valiososos que complementan el contenido central: (1) Selected stated and federal computer crime statues, (2) Citations of state computer crime Statutes, (3) Selected cases reported in the news media, (4) Data processing occupations and their risk in computer technology, (5) Audit tools and techniques, (6) Computer intrusion and contingency and recovery guidelines, (7) Advance preparations and the actual search, (8) Time-sharing usage examples y (9) Directories and databases for contacting expert witnesses.

Poco tiempo después, la abogada Susan Hubell Nycum[128] elaboró un documento de trabajo sobre cuestiones legales relacionadas al abuso informático, el cual fue dirigido al *US Senate Committee on Government Operations in the Committees study of Computer Security in Federal Programs*, entre 1976 y 1977[129]. La conclusión de la autora fue clara y contundente:

> El rápido desarrollo de la tecnología informática proporciona al perpetrador la capacidad de cometer un mal para el que la presente legislación puede no tener remedio. La legislación cuidadosamente redactada a nivel federal y estatal puede ser la única manera de combatir eficazmente el crimen en un entorno computarizado. Con suerte, los legisladores estatales considerarán introducir y apoyar una legislación similar a la propuesta por el senador Ribicoff a nivel federal para llenar los vacíos en las leyes estatales[130].

Durante este periodo, la labor de Edward H. Coughran[131] también destacó, ya que no solo fue el director del *Computer Center* de la Universidad de California, sino que, además, organizó un simposio para fiscales sobre los delitos informáticos en 1976.

Finalmente, entre los investigadores que sentaron las bases para el desarrollo de legislaciones locales y marcos normativos internacionales que en-

128 Susan Hubbell Nycum trabajó junto a Donn B. Parker. Fue coautora de *Computers and the Law* (1975). Miembro de la junta directiva de la Computer Law Association y vicepresidente de la American Bar Association, sección de Ciencia y Tecnología.

129 En esta época, la Oficina General de Contabilidad de Estados Unidos emitió tres reportes sobre los problemas generados por la tecnología: "Improvements Needed in Managing Automated Decision-making by Computers Throughout The Federal Government" y "Computer-Related Crimes in Federal Programs" del 23 de abril de 1976 y "Managers Need to Provided Better Protection For Federal Automatic Data Processing" del 10 de mayo de 1976. Estos informes fueron enviados al senador Abe Ribicoff. Ver: Schjolberg, *The history of cybercrime*, cit., pp. 20 y s.

130 Nycum, Susan Hubell. "Legal problems of computer abuse". En: *Washington University Law Review* 3, 1977. https://journals.library.wustl.edu/lawreview/article/2231/galley/19064/view/.

131 Autor de *Computer Abuse and Criminal Law* (San Diego: University of California, 1976).

frentasen la cibercriminalidad tenemos, entre otros, a Brandt Allen[132], August Bequai[133], Jay J. Becker[134], Thomas Whiteside[135] y Ulrich Sieber[136] -profesor de la Universidad de Friburgo quien colaboró con diferentes organizaciones internacionales, entre ellas, la Organización para la Cooperación y el Desarrollo Económico y las Naciones Unidas-.

2.3. ESTADOS PIONEROS QUE INCORPORARON LOS DELITOS INFORMÁTICOS EN LA LEGISLACIÓN LOCAL

A continuación, se analizarán las normas iniciales adoptadas por 12 países en su esfuerzo por enfrentar la creciente amenaza de la ciberdelincuencia. En este examen, se precisará el año de creación o de inclusión de dichas normas en los respectivos marcos legales nacionales, así como se ofrecerá un comentario sobre las modificaciones iniciales que se implementaron para adaptarse a los retos emergentes en el ámbito digital. Esta síntesis busca proporcionar una comprensión integral de cómo estos países comenzaron a estructurar su respuesta jurídica frente a un novedoso fenómeno delictivo.

132 Autor de "Embezzlers guide to the computer" (en *Harvard Business Review*, julio-agosto, 1975).

133 Autor de (*Legal Problems in Prosecuting Computer Crimes*. Security Management, 1974).

134 Autor de *Prosecutors Combat Unique Computer Abuse Criminals* (Prosecutor's Brief, agosto, 1977).

135 Autor de "Annals of Crime – Dead Souls in the Computer", en *The New Yorker*, agosto, 1977.

136 De todas sus publicaciones, recomiendo especialmente el trabajo formulado como parte de un acuerdo entre la Universidad de Würzburg y la Comisión Europea (DG XIII), titulado *Legal Aspects of Computer-Related-Crime in the Information Society – COMCRIME - STUDY*, publicado en enero de 1998. La importancia del profesor Siber en la reforma legislativa se ve claramente destacada en: MÖHRENSCHLAGER, Manfred E. "El nuevo derecho penal informático en Alemania". En: MIR PUIG, Santiago (coord.). *Delincuencia informática*. Barcelona: PPU, 1992, pp. 103-106.

Estado	Año	Ordenamiento	Comentario
Suecia	1973	Data Protection Act	El art. 21 del Acta de Protección de Datos sancionó, por primera vez, las conductas ilícitas cometidas contra cualquier tipo de datos: "Cualquier persona que sin autorización asegure el acceso a una grabación para el procesamiento de datos electrónicos, altere, elimine o agregue a dicha grabación, será sentenciada por violación de datos a pagar una multa o a prisión de no más de 2 años, a menos que el delito sea punible en el Código Penal, ya que la grabación también se considera información que se transfiere a través de una ayuda electrónica o similar para ser utilizada para el procesamiento electrónico de datos [...]".
Alemania	1980	Código Penal	La legislación alemana incluyó nuevos tipos penales en el Código Penal: La sección 263-A sancionó el fraude informático en los siguientes términos: "Quien procura para sí o para tercero cualquier ventaja ilegal de la propiedad, cause perjuicio a la propiedad de otro al influir en el resultado de una actividad de procesamiento de datos relacionados con la propiedad mediante el uso de datos falsos, o la distorsión o supresión de datos verdaderos, o al afectar el flujo del programa, será sancionado a prisión no mayor a cinco años o a una multa, a menos que el delito sea punible bajo la Sec. 263". La sección 269 recogió el delito de atentado contra los datos informáticos: "Cualquier persona que, con el fin de defraudar en transacciones legales, altere, sin la debida autoridad, cualquier dato almacenado electrónicamente, magnética o de otra manera invisible, que, cuando se procesen en transacciones legales, estén destinados a ser utilizados como evidencia de asuntos de hecho legalmente relevantes, o utilice dichos datos así alterados, será sentenciado a prisión de no más de cinco años o a una multa". Finalmente, la sección 270 prevé que "cualquier manipulación fraudulenta de un sistema informático constituye una defraudación".
Reino Unido	1981	The Counterfeit and Forgery Act	La Ley de Falsificación de 1981 castigó a los delincuentes informáticos que ingresaran información falsa o alterasen cualquier soporte. Así, se definió el objeto de falsificación en el art. 8 (1) (d): "Cualquier disco, cinta, pista de sonido u otro dispositivo en el que la información se grabe o almacene por medios mecánicos, electrónicos o de otro tipo".
Canadá	1985	Criminal Law Amendment	El art. 342.1 (1) estableció lo siguiente: "Todo aquel que, fraudulentamente y sin derecho, (a) obtenga, directa o indirectamente, cualquier servicio informático, (b) por medio de un dispositivo electromagnético, acústico, mecánico o de otro tipo, intercepta o hace que se intercepta, directa o indirectamente, cualquier función de un sistema informático, (c) utiliza o hace que se utilice, directa o indirectamente, un sistema informático con la intención de cometer un delito bajo los parágrafos (a) o (b) o un delito en virtud del artículo 430 en relación con datos o sistemas informáticos, es culpable de un delito sancionado con una pena no mayor a 10 años de prisión, o es culpable de un delito sancionado con una condena sumaria".
Dinamarca	1985	Código Penal	Dinamarca incorporó en su legislación penal dos delitos informáticos en 1985: 193 (1): "Cualquier persona que cause ilegalmente perturbaciones importantes en el funcionamiento de los medios públicos de comunicación, de los servicios públicos de correo, de los servicios telegráficos o telefónicos de uso público, de las instalaciones de radio y televisión, de los sistemas de procesamiento de datos o las instalaciones para el suministro público de agua, gas, electricidad o calefacción será susceptible de detención simple o prisión por un periodo no mayor a 4 años o, en circunstancias atenuantes, a una multa". 263 (2): "Cualquier persona que obtenga ilegalmente acceso a la información o programas de otra persona diseñados para ser utilizados en relación con el procesamiento electrónico de datos, estará sujeta a una multa, a detención simple o a prisión por un periodo no mayor a 6 meses".

Estado	Año	Ordenamiento	Comentario
Estados Unidos	1986	The Counterfeit Access Device and Computer Fraud and Abuse Act	El 16 de octubre de 1986, se suscribió la primera legislación federal especializada en delincuencia informática, titulada "Ley de acceso a dispositivos, fraude informático y abuso". Esta norma sanciona el acceso ilícito, así como diferentes tipos de fraudes en los que se emplean dispositivos informáticos[137].
Austria	1987	Criminal Law Amendment Act 1987	Austria incorporó el art. 126-A al Código Penal para sancionar los atentados contra datos informáticos en los siguientes términos: (1) Una persona que cause daños a otra persona al alterar, borrar o inutilizar o suprimir automáticamente los datos procesados, transmitidos o confiados sin estar autorizada a deshacerse de los datos o a deshacerse de ellos solos, será condenada a prisión de hasta 6 meses o a pagar multas de hasta 360 días. (2) Los datos personales y los datos no personales, así como los programas informáticos, deben entenderse como datos en el sentido del párrafo 1. (3) Una persona que cause daños superiores a 25 000 AS por este delito será condenada a prisión de hasta dos años o a pagar una multa de hasta 360 días, una persona que cause daños superiores a 500 000 AS será condenada a prisión de 6 meses a 5 años.
Japón	1987	Código Penal	La reforma del Código Penal japonés incluyó el término *registro electromagnético*, definiéndolo en el art. 7-2 como "cualquier registro que es producido por medios electromagnéticos o cualquier otro que es irreconocible por funciones naturales de percepción y es usado para el procesamiento de datos por computadoras". Entre otras normas, se incluyó la obstrucción de negocios por la destrucción informática. Así, el art. 234-2 estableció: "Una persona que obstruye el negocio de otra impidiendo que el funcionamiento de una computadora sea utilizado para el propósito del negocio o que opere de una manera contradictoria a su finalidad, mediante la destrucción de la computadora, un registro electromagnético, o proveyéndole información o un comando falso, o de alguna otra manera, será castigado con castigo laboral no mayor a 5 años y una multa no mayor a 400 mil yenes".
Noruega	1987	Código Penal	El art. 145 (2) del Código Penal se modificó en los siguientes términos: "La misma pena se aplica a quien quiebre un dispositivo protector o, de forma similar, ilegalmente obtiene acceso a datos o programas que almacenan o transfieren electrónicamente o de forma técnica".
Francia	1988	Código Penal	El delito de "*la fraud informatique*", previsto en el art. 462-2 del Código Penal francés fue modificado como sigue: "Toda persona que acceda fraudulentamente o haga uso de un sistema de procesamiento automático de data, o parte de este, será condenado a no menos de dos meses ni más de un año, y una multa de 2000 a 50 000 francos, o uno de los dos castigos". "Cuando el delito ocasione la supresión o alteración de data de un sistema, o la alteración de su funcionamiento, la sanción será no menor de dos meses ni más de dos años y una multa de 10 000 a 100 000 francos".

137 Como se ha señalado anteriormente, los esfuerzos legislativos en Estados Unidos iniciaron en 1976-1977 con tres reportes remitidos por la Oficina General de Contabilidad al senador Rubicoff.

Estado	Año	Ordenamiento	Comentario
Grecia	1988	Código Penal	El Código Penal griego se modificó para incluir los delitos informáticos. Así, el art. 370-C sancionó la siguiente conducta: "1. Toda persona que, sin derecho, copie o utilice programas informáticos será castigada con prisión no mayor a 6 meses y con sanción pecuniaria de 100 a 2 millones de dracmas". "2. Toda persona que obtenga acceso a datos registrados en un ordenador o en la memoria externa de un ordenador o transmitidos por sistemas de telecomunicaciones será castigado con prisión de hasta 3 meses o con una sanción pecuniaria de no menos de 10 mil dracmas, a condición de que estos actos se hayan cometido sin derecho, especialmente en violación de las prohibiciones o de las medidas de seguridad adoptadas por el titular legal. Si el acto se refiere a las relaciones internacionales o a la seguridad del Estado, será castigado de conformidad con el art. 148". "3. Si el delincuente está al servicio del titular legal de los datos, el acto del párrafo anterior se castigará solo si ha sido explícitamente prohibido por regulaciones internas o por una decisión escrita del titular o de un empleado competente suyo [...]".
Australia	1989	Ley de Delitos de la Commonwealth	Australia incorporó los siguientes artículos en 1989: "Art. 76-B.- Acceso ilegal a los datos en la Commonwealth y otros ordenadores. 76B (1). Una persona que intencionalmente y sin autoridad obtiene acceso a: datos almacenados en un ordenador de la Commonwealth o datos almacenados en nombre de la Commonwealth en un ordenador que no sea un ordenador de Commonwealth, es culpable de un delito. Pena: Encarcelamiento por 6 meses". "Art. 76-C.- Daños de datos en Commonwealth y otras computadoras. 76C. Una persona que intencionalmente y sin autoridad o excusa legal: destruye, borra o altera los datos almacenados o inserta datos en una computadora de la Commonwealth; interfiere con, o interrumpe u obstruye el uso legal de, una computadora de la Commonwealth; destruye, borra, altera o agrega a los datos almacenados en nombre de la Commonwealth en un ordenador que no es un ordenador del Commonwealth; o impide o impide el acceso a, o perjudica la utilidad o eficacia de, los datos almacenados en una computadora de la Commonwealth o los datos almacenados en nombre de la Commonwealth en una computadora que no es una computadora de la Commonwealth; es culpable de un delito. Pena: Encarcelamiento por 10 años". "Art. 76-D.- Acceso ilegal a los datos en el Commonwealth y otros ordenadores por medio de las instalaciones del Commonwealth. 76D (1). Una persona que, por medio de una instalación operada o proporcionada por el Commonwealth, obtenga acceso intencional y sin autoridad a los datos almacenados en un ordenador es culpable de un delito. Pena: Encarcelamientos por 6 meses".

Cuadro 6. Legislación comparada inicial (1973 a 1989). Elaboración propia[138].

A continuación, se realizará un recuento de los principales encuentros y el marco normativo más relevante adoptado para enfrentar la ciberdelincuencia en los sistemas europeos y americanos, culminando con un estudio del enfoque establecido por las Naciones Unidas en esta materia. El análisis seguirá un orden cronológico, lo que permitirá apreciar la evolución y el desarrollo de las nor-

138 La información fue obtenida de Schjolberg, *The history of cybercrime*, cit., pp. 25-32 (traducción propia).

mativas en cada región. Asimismo, se resaltarán los aspectos más importantes y distintivos, con el objetivo de proporcionar una visión integral de los esfuerzos internacionales en esta lucha.

2.4. SISTEMA EUROPEO[139]

2.4.1. Conferencia sobre aspectos criminológicos de los delitos económicos, 1976

La expresión *delito informático* -o *computer crime*, en inglés- fue utilizada por el Consejo de Europa, por primera vez, en la 12 Conferencia de directores del Instituto de Investigación Criminológica: Criminological Aspects of Economic Crimes, celebrada entre el 15 y el 18 de noviembre de 1976 en Estrasburgo, Francia. Así, dicha expresión fue definida como:

> Any illegal action in which a computer is a tool or object of the crime, in other words any crime the means or purpose of which is to influence the function of a computer [Cualquier acción ilegal en la que una computadora es una herramienta u objeto del delito, es decir, cualquier delito cuyo medio o propósito es influir en el funcionamiento de una computadora] [140].

139 En doctrina, se reconoce que la política europea no ha sido reactiva a ciberataques concretos sino que ha evolucionado de manera progresiva: "[...] a diferencia de otras políticas de la Unión, como la antiterrorista, la actuación de la UE en este ámbito no ha sido reactiva, de respuesta a ciberataques concretos, sino que ha evolucionado en el marco de una estrategia de ciberseguridad que se ha ido construyendo de forma paulatina y cada vez más decidida, a medida que la amenaza cibernética se ha ido haciendo más patente. Los ciberataques a gran escala que sufrieron Estonia, Lituania y Georgia en 2007 y 2008 contribuyeron a resaltar la gravedad de un problema creciente, y la persistencia de esta amenaza ha contribuido a mantener en la agenda de las instituciones europeas la necesidad de desarrollar una política de ciberseguridad integral. De hecho, aún en 2010 se dudaba de si la UE debía tener un papel que jugar en ese ámbito habida cuenta de que la seguridad nacional es responsabilidad de los Estados miembros, debate que en la actualidad está completamente superado al reconocerse a la Unión Europea un importante en materia de ciberseguridad" (Piernas López, Juan Jorge. "La respuesta de la Unión Europea a las amenazas del ciberespacio". En: Cervell Hortal, María José [dir.)]. *Nuevas tecnologías en el uso de la fuerza: Drones, armas autónomas y ciberespacio*. Navarra: Thomson Reuters / Aranzadi, 2020, p. 305).

140 Schjolberg, *The history ob cybercrime*, cit., p. 32.

2.4.2. Convenio N.º 108 del Consejo de Europa, para la protección de personas con respecto al tratamiento informatizado de datos personales, 1981

El 28 de enero de 1981, los Estados miembros del Consejo de Europa suscribieron el Convenio para la protección de personas con respecto al tratamiento automatizado de datos de carácter personal. Ya en esta temprana época se destacaba la importancia de la seguridad de los datos. Así, en los arts. 7 y 10 se estableció lo siguiente:

> Art. 7. Se tomarán medidas de seguridad apropiadas para la protección de datos de carácter personal registrados en ficheros automatizados contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados.
>
> Art. 10. Cada Parte se compromete a establecer sanciones y recursos convenientes contra las infracciones de las disposiciones de derecho interno que hagan efectivos los principios básicos para la protección de datos enunciados en el presente capítulo.

Como se puede apreciar, se sugiere que los Estados adopten las medidas necesarias para minimizar el riesgo de la confidencialidad (acceso y difusión), así como la disponibilidad e integridad de los datos (destrucción y modificación) o, llegado el caso, sancionar eficazmente las infracciones (delitos) que se cometan contra estos.

2.4.3. Recomendaciones de la OCDE, 1986

La OCDE invitó a un grupo de especialistas a discutir sobre los delitos informáticos y la necesidad de efectuar cambios o modificaciones en los diferentes códigos penales de la región. Este grupo, conocido como *los fundadores* de la armonización de la legislación europea en delitos informáticos, se reunió en París, en mayo de 1983, recomendando la adopción de un comité de expertos.

En esta época, la OCDE empleó la siguiente definición: "El delito relacionado con sistemas de cómputo es considerado como cualquier comportamiento

ilícito, no ético y no autorizado que involucra el procesamiento automatizado y la transmisión de datos"[141].

El comité de expertos presentó sus recomendaciones en setiembre de 1985. Seleccionaron y recomendaron una lista de delitos que tenían bases similares: fraude informático, falsificación informática, atentados contra datos informáticos y programas, infracción no autorizada de programas informáticos protegidos, acceso e interceptación ilícita de sistemas informáticos.

Como resultado de la propuesta del comité de expertos, a través de la Dirección de Ciencia, Tecnología e Industria, el comité de la OCED recomendó en 1986 lo siguiente:

> With respect to the transnational aspects of computer-related criminal activity, important issues have been noted which point to the desirability for international cooperation in repressing and controlling such activity. And that all member countries consider the extent to which acts committed knowingly in this field should be covered by national penal legislation. These acts may be expressed as far as possible in terms of functions rather than technology [Con respecto a los aspectos transnacionales de la actividad delictiva relacionada con computadoras, se han señalado importantes problemas que apuntan a la conveniencia de la cooperación internacional para reprimir y controlar tales actividades. Asimismo, todos los países miembros deberían considerar hasta qué punto los actos cometidos de manera consciente en este ámbito deben ser previstos por la legislación penal nacional. Estos actos podrían expresarse, en la medida de lo posible, en términos de funciones en lugar de tecnología][142].

2.4.4. Recomendaciones del Consejo de Europa, 1989

Según el profesor Enrique Rovira, la criminalidad informática comenzó a ser tomada con mayor seriedad en Europa a partir de 1985. En este contexto,

---

141 Villanueva, Ernesto y Vanessa Díaz. *Derecho de las nuevas tecnologías (en el siglo XX derecho informático).* Ciudad de México: Oxford University Press Mexico, 2015, pp. 66 y s.

142 Cfr. Villanueva y Díaz, *Derecho de las nuevas tecnologías (en el siglo XX derecho informático),* cit., p. 37.

el programa del Comité Europeo, integrado por expertos de los trece Estados miembros y tres independientes, abordó la problemática de los delitos vinculados al uso de computadoras[143].

De este modo, el Comité Selecto de Expertos en Delitos Informáticos del Consejo de Europa presentó en marzo de 1989 la Recomendación N.° R (89) 9, la cual establecía una serie de directrices para que los legisladores nacionales sancionaran los delitos informáticos dolosos. Esta recomendación incluía tanto una lista mínima de delitos que debían ser penalizados como una lista opcional[144].

En la lista mínima de delitos, encontramos: (1) Fraude informático[145], (2) falsificación informática[146], (3) daño a los datos o programas informáticos[147], (4) sabotaje informático[148], (5) acceso ilícito[149], (6) interceptación no autorizada[150],

143 Rovira Del Canto, Enrique. *Delincuencia informática y fraudes informáticos*. Granada: Editorial Comares, 2002, p. 292.

144 A continuación, transcribo las propuestas normativas en su idioma original, pues son muy similares a las que actualmente rigen los diferentes ordenamientos -incluido, el peruano-.

145 "The input, alteration, erasure or suppression of computer data or computer programs, or other interference with the course of data processing, that influences the result of data processing thereby causing economic or possessory loss of property of another person with the intent of procuring an unlawful gain for himself or for another person (alternative draft: with the intent to unlawfully deprive that person of his property". Ibid. p. 38.

146 "The input, alteration, erasure o suppression of computer data or computer programs, or other interference with the course of data processing, in a manner or under such conditions, as prescribed by national law, that it would constitute the offence of forgery if it had been committed with respect to a traditional object of such an offence". Idem.

147 "The erasure, damaging, deterioration or suppression of computer data or computer programmes without right". Ibid. p. 39.

148 "The input, alteration, erasure or suppression of computer data or computer programs, or interference with computer systems, with the intent to hinder the functioning of a computer or a telecommunication system". Idem.

149 "The access without right to a computer system or network by infringing security measures". Idem

150 "The interception, made without right and by technical means, of communications to, from and within a computer system or network". Idem.

(7) reproducción no autorizada de programas informáticos protegidos[151] y (8) reproducción no autorizada de una topografía[152].

De otro lado, en la lista opcional, se recomendó lo siguiente: (1) alteración de datos o programas informáticos[153], (2) espionaje informático[154], (3) uso no autorizado de un sistema informático[155] y (4) uso no autorizado de programas informáticos protegidos[156].

Este episodio generó interés, pero también preocupación entre juristas y especialistas en la materia, pues, en Alemania, por ejemplo, se intentó evitar la sobrecriminalización y buscar salidas alternativas para resolver el conflicto:

> Una comisión de expertos del Consejo de Europa continúa desde finales de 1985 los trabajos de la OCDE, teniendo por objeto la presentación de un informe. Esta comisión ha revisado de nuevo, completado y en parte modificado, las recomendaciones de la OCDE. Además, diferencia con más detalle entre aquellas acciones que deben ser conminadas con pena en los Estados miembros (la llamada Lista Mínima) y aquellas en las que ello es dejado al libre criterio de los mismos (la

151 "The reproduction, distribution or communication to the public without right of a computer program, which is protected by law". Idem.

152 "The reproduction without right of a topography, protected by law, of a semi-conductor product, or the commercial exploitation or the importation for that purpose, done without right, of a topography or of a semi-conductor product manufactured by using the topography". Idem.

153 "The alteration of computer data or computer programs without right". Idem.

154 "The acquisition by improper means or the disclosure, transfer or use of a trade or commercial secret without right or any other legal justification, with the intent either to cause economic loss to the person entitled to the secret or to obtain an unlawful economic advantage for oneself or a third person". Idem.

155 "The use of a computer system network without right, that either: a) is made with the acceptance of a significant risk of loss being caused to the person entitled to use the system or harm to the system or its functioning, or b) to made with the intent to cause loss to the person entitled to use the system or harm to the system or its functioning, or c) causes loss to the person entitled to use the system or harm to the system or it's functioning". Idem.

156 "The use without right of a computer program which is protected by law and which has been reproduced without right, with the intent, either to procure and unlawful economic gain for himself or for another person or cause harm to the holder of the right". Ibid. p. 40.

> Lista Operativa o Facultativa). Y, asimismo, las recomendaciones deberán ser dotadas de un comentario más pormenorizado y el informe se completará con referencias a aspectos internacionales. Entre tanto, el Consejo de Europa ya ha presentado una recomendación para el ámbito de la llamada "piratería" informática -el uso y copia ilícitos de programas protegidos de ordenador -en relación con la llamada "piratería" de vídeo.
>
> [...]
>
> El legislador alemán ha introducido un número relativamente alto de nuevos preceptos penales, pero no ha llegado tan lejos como, p. ej., los EE. UU. Así, no solo ha renunciado a tipificar la mera penetración no autorizada en sistemas ajenos de computadoras, sino que tampoco ha castigado el uso no autorizado de equipos de proceso de datos, aunque tenga lugar de forma cualificada. Han motivado esta actitud de prudencia el temor a una "sobre-incriminación", la impunidad del *furtum usus* en Derecho alemán y las posibilidades de reparación civil del daño, así como de despido de los empleados infieles. El legislador de cada país -también el español- debe decidir por sí mismo donde ha de trazar las fronteras del Derecho penal en esta materia [...][157]

2.4.5. Recomendaciones del Consejo de Europa, 1995[158]

El 11 de setiembre de 1995, el Comité de ministros del Consejo de Europa adoptó la Recomendación N.º R (95) 13, *Problemas relevantes del Derecho Procesal Penal relacionado con las Tecnologías de Información.*

La Recomendación introduce 18 principios divididos en 7 capítulos, los cuales fueron sugeridos a los estados miembros: (1) búsqueda e incautación, (2) vigilancia técnica, (3) obligación de cooperar con las autoridades investigadoras, (4) evidencia electrónica, (5) uso de encriptación, (6) búsqueda, estadística y entrenamiento, y (7) cooperación internacional[159].

---

157 Möhrenschlager, Manfred E. "Tendencias en política jurídica en la lucha contra la delincuencia relacionada con la Informática". En: Mir Puig, Santiago (coord.). *Delincuencia informática*. Barcelona: PPU, 1992, pp. 51 y 64.

158 Rovira Del Canto, *Delincuencia informática y fraudes informáticos*, cit., pp. 301 y s.

159 Ibid., pp. 40-43.

Como se puede apreciar, la necesidad de mejorar las investigaciones tecnológicas para la obtención y aseguramiento de la prueba digital generaba preocupación e interés entre los estados miembros del Consejo de Europa.

2.4.6. Protocolo adicional al Convenio N.° 108, relativo a autoridades de supervisión y flujos internacionales de datos, 2001

Tomando en consideración el incremento o aumento del intercambio de datos personales a través de las fronteras, devino en necesario la creación de autoridades de control. De este modo, el 8 de noviembre de 2001 se estableció que cada Estado debía contar con una o más autoridades responsables de asegurar la conformidad de las medidas oportunas que den cumplimiento en el Derecho Interno a los principios contenidos en los capítulos II y III del Convenio N.° 108.

2.4.7. Convenio sobre la Ciberdelincuencia, 2001

El Convenio sobre la Ciberdelincuencia o Convenio de Budapest es el principal instrumento internacional en la lucha contra este fenómeno delictivo. Junto a su informe explicativo, fue aprobado por el comité de miembros del Consejo de Europa en su 109ª reunión, celebrada el 08 de noviembre del 2001, y abierto a la firma en Budapest, el 23 de noviembre del 2001, con motivo de la celebración de la Conferencia Internacional sobre la Ciberdelincuencia[160].

160 "El Convenio de Budapest es el resultado de cuatro años de trabajo previo de los expertos de los 45 países miembros del Consejo de Europa y de no miembros como Estados Unidos, Canadá y Japón. Su negociación coincidió con el auge del comercio electrónico, a la propiedad intelectual y la mayor penetración del acceso de banda ancha a Internet y de la telefonía móvil" (Barrio Andrés, *Delitos 2.0. Aspectos penales, procesales y de seguridad de los ciberdelitos*, cit., pp. 59 y s.). "El Convenio es un instrumento que sirve como referente para una política común a nivel mundial frente a la lucha contra la ciberdelincuencia, si bien, en muchas ocasiones colisiona con la normatividad interna de los países que se han adherido" (Ortiz Hernández, Susana. "La regulación de los delitos con origen tecnológico". En: Garrós Font, Imma y otros. *Delitos cibernéticos: amenazas digitales del siglo XXI. Análisis normativo, psicológico y criminológico*. Navarra: Thomson Reuters / Aranzadi, 2023, p. 33).

El convenio tiene como finalidad primordial los siguientes objetivos -los cuales se desarrollan en el párrafo 16 del informe explicativo-[161]:

a. Armonizar los elementos de los delitos conforme al derecho sustantivo penal de cada país y las disposiciones conexas en materia de delitos informáticos[162].

b. Establecer conforme al derecho procesal de cada país los poderes necesarios para la investigación y el procesamiento de dichos delitos, así como también de otros delitos cometidos mediante el uso de un sistema informático o las pruebas conexas que se encuentren en formato electrónico[163].

---

161 Además del impacto directo, el Convenio ha demostrado su influencia indirecta, en línea con el G-8 y con la Unión Europea, en otros instrumentos multinacionales y en la legislación local (Brodowski, Dominik. *Cibercrimen y protección de la seguridad informática*. Buenos Aires: Ad-Hoc, 2021, p. 35).

162 La sección dedicada al derecho penal sustantivo del Convenio no sólo aborda el catálogo de ciberdelitos cuya tipificación se recomienda sino también la responsabilidad penal de las personas jurídicas. Sobre este tópico, ver: Riquert, Marcelo A. "La responsabilidad penal de las personas jurídicas en Argentina y el ciberconvenio de Budapest". En: Dupuy, Daniela (dir.). *Cibercrimen II. Nuevas conductas penales y contravencionales. Inteligencia artificial aplicada al derecho penal y procesal penal. Novedosos medios probatorios para recolectar evidencia digital. Cooperación internacional y victimología*. Montevideo: B de F, 2018, pp. 443-482.

163 Algunos autores resaltan la necesidad de que los Estados miembro adecúen su legislación procesal para combatir eficazmente la cibercriminalidad. Así, por ejemplo, sobre el análisis forense durante el allanamiento, se resalta que es "necesario concluir además que, de acuerdo a la Convención de Budapest, este tipo de procedimientos debería ser incluido expresamente en la normativa procesal; concretamente, el art. 19 del convenio trata los lineamientos generales que se deben tener en cuenta en relación a qué tratamiento brindar a los datos informáticos, ya sean de un sistema informático o parte de él, como también contempla el régimen de todo dispositivo de almacenamiento informático que permita almacenar datos informáticos [...] En suma, la regulación del análisis en el lugar del allanamiento es un hecho, y quedará en manos de los legisladores correspondientes el tratamiento que se le dará de acuerdo a las posibilidades técnicas, la práctica judicial y las previsiones de la Convención de Budapest" (Fusalba, Joana y Javier Martín López Zavaleta. "Los registros domiciliarios con análisis de dispositivos de almacenamiento de datos en el lugar. Qué ocurre en las investigaciones de delitos que involucran la integridad sexual de menores. Realidad judicial y la implicancia de la adhesión de la República de Argentina al Convenio de Budapest sobre ciberdelincuencia. Necesidad de reformas procesales". En: Dupuy, Daniela [dir.] y Mariana Kiefer [coord.]. *Cibercrimen II. Nuevas conductas penales y contravencio-*

c. Establecer un régimen rápido y eficaz de cooperación internacional[164].

En cuanto a su estructura, el Convenio de Budapest está dividido en cuatro capítulos, que recogen 48 artículos -los cuales, a su vez, han sido desarrollados en 330 parágrafos del informe explicativo-.

Capítulo	Artículos del Convenio de Budapest		Parágrafos del inf. explicativo
Cap. I Terminología	Art. 1. Definiciones		Par. 22-31
Cap. II. Medidas que deberán adaptarse a nivel nacional	Secc. 1	Derecho penal sustantivo	Par. 33-42
	Título 1	Delitos contra la confidencialidad, la integridad y la disponibilidad y sistemas informáticos	Par. 43
	Art. 2.	Acceso ilícito	Par. 44-50
	Art. 3.	Interceptación ilícita	Par. 51-59
	Art. 4.	Ataques a la integridad de los datos	Par. 60-64
	Art. 5.	Ataques a la integridad del sistema	Par. 65-70
	Art. 6.	Abuso de los dispositivos	Par. 71-78
	Título 2	Delitos informáticos	Par. 79-80
	Art. 7.	Falsificación informática	Par. 81-85
	Art. 8.	Fraude informático	Par. 86-90
	Título 3	Delitos relacionados con el contenido	-
	Art. 9.	Delitos relacionados con la pornografía infantil	Par. 91-106
	Título 4	Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines	-
	Art. 10.	Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines	Par. 107-117
	Título 5	Otras formas de responsabilidad y de sanción	-
	Art. 11.	Tentativa y complicidad	Par. 118-122

nales. Inteligencia artificial aplicada al derecho penal y procesal penal. Novedosos medios probatorios para recolectar evidencia digital. Cooperación internacional y victimología. Montevideo: B de F, 2018, pp. 217 y s).

164 "Exponen también los Estados signatarios que el Convenio resulta necesario para prevenir los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos, mediante la tipificación de esos actos, tal y como se definen en el propio Convenio, y la asunción de poderes suficientes para luchar de forma efectiva contra dichos delitos, facilitando su detección, investigación y sanción, tanto a nivel nacional como internacional, y estableciendo disposiciones que permitan una cooperación internacional rápida y fiable" (Davara Fernández de Marcos, Elena y Laura Davara Fernández de Marcos [coords.]. *Delitos informáticos*. Navarra: Thomson Reuters / Aranzadi, 2017, p. 239).

Capítulo	Artículos del Convenio de Budapest	Parágrafos del inf. explicativo
Cap. II. Medidas que deberán adaptarse a nivel nacional	Art. 12. Responsabilidad de las personas jurídicas	Par. 123-127
	Art. 13. Sanciones y medidas	Par. 128-130
	Secc. 2 Derecho procesal	Par. 131-138
	Título 1 Disposiciones comunes	Par. 139
	Art. 14. Ámbito de aplicación de las disposiciones de procedimiento	Par. 140-144
	Art.15. Condiciones y salvaguardas	Par. 145-148
	Título 2 Conservación rápida de datos informáticos almacenados	Par. 149-157
	Art. 16. Conservación rápida de datos informáticos almacenados	Par. 158-164
	Art. 17. Conservación y revelación parcial rápidas de los datos relativos al tráfico	Par. 165-169
	Título 3 Orden de presentación	-
	Art. 18. Orden de presentación	Par. 170-183
	Título 4 Registro y confiscación de datos informáticos almacenados	-
	Art. 19. Registro y confiscación de datos informáticos almacenados	Par. 184-204
	Título 5 Obtención en tiempo real de datos informáticos	Par. 205-215
	Art. 20. Obtención en tiempo real de datos relativos al tráfico	Par. 216-227
	Art. 21. Interceptación de datos relativos al contenido	Par. 228-231
	Secc. 3 Jurisdicción	-
	Art. 22. Jurisdicción	Par. 232-239
Cap. III. Cooperación internacional	Secc. 1 Principios generales	-
	Título 1 Principios generales relativos a la cooperación internacional	-
	Art. 23. Principios generales relativos a la cooperación internacional	Par. 241-244
	Título 2 Principios relativos a la extradición	-
	Art. 24. Extradición	Par. 245-252
	Título 3 Principios generales relativos a la asistencia mutua	-
	Art. 25. Principios generales relativos a la asistencia mutua	Par. 253-259
	Art. 26. Información espontánea	Par. 260-261
	Art. 27. Procedimientos relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables	Par. 262-274
	Título 4 Procedimientos relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables	-
	Art. 28. Confidencialidad y restricciones de uso	Par. 275-280
	Secc. 2 Disposiciones específicas	Par. 281
	Título 1 Asistencia mutua en materia de medidas provisionales	-
	Art. 29. Conservación rápida de datos informáticos almacenados	Par. 282-289
	Art. 30. Revelación rápida de datos conservados	Par. 290-291
	Título 2 Asistencia mutua en relación con los poderes de investigación	-
	Art. 31. Asistencia mutua en relación con el acceso a datos almacenados	Par. 292
	Art. 32. Acceso transfronterizo a datos almacenados, con consentimiento o cuando sea accesible al público	Par. 293-294

Capítulo	Artículos del Convenio de Budapest		Parágrafos del inf. explicativo
Cap. III. Cooperación internacional	Art. 33.	Asistencia mutua para la obtención en tiempo real de datos relativos al tráfico	Par. 295-296
	Art. 34.	Asistencia mutua en relación con la interceptación de datos relativos al contenido	Par. 297
	Título 3	Red 24/7	-
	Art. 35.	Red 24/7	Par. 298-302
Cap. IV. Cláusulas	Art. 36.	Firma y entrada en vigor	Par. 304-305
	Art. 37.	Adhesión al Convenio	Par. 306-307
	Art. 38.	Aplicación territorial	-
	Art. 39.	Efectos del Convenio	Par. 308-314
	Art. 40.	Declaraciones	Par. 315
	Art. 41.	Cláusula federal	Par. 316-319
	Art. 42.	Reservas	Par. 320
	Art. 43.	Mantenimiento y retirada de las reservas	Par. 321-322
	Art. 44.	Enmiendas	Par. 323-325
	Art. 45.	Solución de controversias	Par. 326
	Art. 46.	Consulta entre las Partes	Par. 327-330
	Art. 47.	Denuncia	-
	Art. 48.	Notificación	-

Cuadro 7: Cuadro resumen del Convenio de Budapest y del informe explicativo. Elaboración propia.

Es importante destacar que el convenio ha sido firmado y ratificado por 77 países[165], incluso por países no miembros del Consejo de Europa. A continuación, se detalla la relación de los estados que se han adherido, así como los que han sido invitados a acceder, al 31 de diciembre de 2024[166]:

165 Sobre el contexto en que se desarrolló su aprobación, se recuerda que "este tratado fue una de las primeras respuestas a los ataques que habrían ocurrido en Nueva York dos meses atrás en el atentado terrorista conocido como el 11-S" (Nava Garcés, Alberto. *Delitos informáticos*. 4.ª edición. México: Porrúa, 2018, p. 147).

166 Council of Europe. *The global state of cybercrime legislation 2013-2024: A cursored overview*, 2025. https://rm.coe.int/3148-1-3-4-cyberleg-global-state-dec-2024-public-v6-final/1680b3ecc5

Estados		Invitados a firmar o acceder
Albania	Islandia	Guatemala
Alemania	Israel	Irlanda
Andorra	Italia	Kazajistán
Argentina	Japón	Kenia
Armenia	Kiribati	Malawi
Australia	Letonia	México
Austria	Liechtenstein	Mozambique
Azerbaiyán	Lituania	Níger
Bélgica	Luxemburgo	Nueva Zelandia
Benín	Macedonia del Norte	Papúa Nueva Guinea
Bosnia y Herzegovina	Malta	República de Corea
Brasil	Mauricio	Ruanda
Bulgaria	Mónaco	Santo Tomé y Príncipe
Cabo Verde	Montenegro	Sudáfrica
Camerún	Marruecos	Timor-Leste
Canadá	Nigeria	Trinidad y Tobago
Chile	Noruega	Uruguay
Colombia	Países Bajos	Vanuatu
Costa Rica	Panamá	
Costa de Marfil	Paraguay	
Croacia	Perú	
Chipre	Polonia	
Dinamarca	Portugal	
República Dominicana	Reunido Unido	
Ecuador	República Checa	
Estonia	República de Eslovaquia	
Eslovenia	República de Moldova	
España	Rumania	
Estados Unidos	San Marino	
Fiyi	Senegal	
Filipinas	Serbia	
Francia	Sierra Leona	
Georgia	Sri Lanka	
Gana	Suecia	
Granada	Suiza	
Grecia	Tonga	
Hungría	Túnez	
	Turquía	
	Ucrania	

Cuadro 8: Estados adherentes e invitados a suscribir el Convenio de Budapest, al 31 de diciembre de 2024.

En América Latina, nueve países lo han ratificado, entrando en vigor con ciertas declaraciones y/o reservas:

País	Fecha de ratificación	Entrada en vigor	Declaraciones y/o reservas
1. Ecuador	04 de julio de 2024	90 días después	Sin información disponible.
2. Brasil	22 de diciembre del 2021	30 de noviembre del 2022	Sin información disponible.
3. Colombia	16 de marzo del 2020	01 de julio del 2020	Una reserva. Tres declaraciones del 16 de marzo del 2020.

País	Fecha de ratificación	Entrada en vigor	Declaraciones y/o reservas
4. Perú	10 de marzo del 2019	01 de diciembre del 2019	Tres reservas. Cuatro declaraciones del 26 de agosto del 2019.
5. Paraguay	30 de julio del 2018	01 de noviembre del 2018	Sin reservas. Tres declaraciones del 30 de julio del 2018.
6. Argentina	05 de junio del 2018	01 de octubre del 2018	Cinco reservas. Dos declaraciones del 05 de junio del 2018.
7. Costa Rica	22 de setiembre del 2017	01 de enero del 2018	Dos reservas. Dos declaraciones del 22 de setiembre del 2017.
8. Chile	20 de abril del 2017	01 de agosto del 2017	Cinco reservas. Dos declaraciones del 20 de abril del 2017.
9. Panamá	05 de marzo del 2014	01 de julio del 2014	Sin reservas. Tres declaraciones del 05 de marzo del 2014.
10. República Dominicana	07 de febrero del 2013	01 de junio del 2013	Sin reservas. Dos declaraciones del 07 de febrero del 2013.

Cuadro 9: Estados latinoamericanos que se adhirieron al Convenio de Budapest, al 2024[167].

2.4.8. Primer Protocolo adicional al Convenio sobre Ciberdelincuencia, relativo a la penalización de actos de naturaleza racista y xenófoba cometidos por medio de sistemas informáticos, 2003

El 28 de enero de 2003 se suscribió el protocolo en referencia. Los Estados miembros del Consejo de Europa y los demás estados parte advirtieron que los sistemas informáticos facilitaban la propaganda racista y xenófoba, pero también eran conscientes de que las legislaciones locales debían ser respetuosas de la libertad de expresión. Intentando lograr un equilibrio, suscribieron un protocolo adicional en el que se conceptualizaba "material racista y xenófobo" y se proponía la tipificación de tres delitos afines: difusión de material racista y xenófobo mediante sistemas informáticos (art. 3[168]), amenazas con motivación

167 Para la elaboración se tomó como referencia: Velasco San Martín/Velázquez, *Aspectos prácticos de los ciberdelitos y la evidencia digital,* cit., p. 81.

168 Primer Protocolo adicional al Convenio sobre Ciberdelincuencia, art. 3.- [...] difundir o poner a disposición del público de otro material racista y xenófobo por medio de un sistema informático.

racista y xenófoba (art. 4[169]) e insultos con motivación racista y xenófoba (art. 5[170]).

> Art. 2. A efectos del presente Protocolo: por "material racista y xenófobo" se entenderá todo material escrito, toda imagen o cualquier otra representación de ideas o teorías, que propugne, promueva o incite al odio, la discriminación o la violencia, contra cualquier persona o grupo de personas, por razón de la raza, el color, la ascendencia o el origen nacional o étnico, así como de la religión en la medida en que ésta se utilice como pretexto para cualquiera de esos factores.

2.4.9. Convenio del Consejo de Europa para la protección de los niños contra la explotación y el abuso sexual, 2007

Conocido también como Convenio de Lanzarote, este instrumento fue suscrito el 25 de octubre de 2007. Los Estados miembros del Consejo de Europa y demás signatarios reconocieron que el mal uso de las TIC exponía a situaciones de explotación y abuso sexual de menores de edad, razón por la cual se necesitaba prevenir y combatir las nuevas modalidades delictivas que el ciberespacio genera y alberga. Por esta razón, sugirió que cada Estado sancione[171] (i) el abuso sexual, (ii) los delitos relativos a la prostitución infantil, (iii) los delitos relativos a la pornografía infantil, (iv) los delitos relativos a la participación de niños en espectáculos pornográficos, (v) la corrupción de niños y (vi) las proposiciones a niños con fines sexuales.

---

169 Primer Protocolo adicional al Convenio sobre Ciberdelincuencia, art. 4.- [...] amenazar, por medio de un Sistema informático, con la comisión de un delito grave, tal como se define en su derecho interno, i) a personas por razón de su pertenencia a un grupo caracterizado por la raza, el color, la ascendencia o el origen nacional o étnico, así como la religión en la medida en que ésta se utilice como pretexto para cualquiera de esos factores, o ii) a un grupo de personas que se distinga por alguna de esas características.

170 Primer Protocolo adicional al Convenio sobre Ciberdelincuencia, art. 5.- [...] insultar en público, por medio de un Sistema informático, i) a personas por razón de su pertenencia a un grupo caracterizado por la raza, el color, la ascendencia o el origen nacional o étnico, así como la religión en la medida en que ésta se utilice como pretexto para cualquiera de esos factores, o ii) a un grupo de personas que se distinga por alguna de esas características.

171 Se utiliza el *nomen iuris* empleado en el Convenio de Lanzarote.

De los diferentes tipos penales propuestos, debo destacar el *grooming* por su novedad y relevancia:

> Art. 23. Cada parte adoptará las medidas legislativas o de otro tipo que sean necesarias para tipificar como delito el hecho de que un adulto, mediante las tecnologías de la información y la comunicación, proponga un encuentro a un niño que no haya alcanzado la edad fijada en aplicación del apartado 2 del artículo 18 con el propósito de cometer contra él cualquiera de los delitos tipificados con arreglo al apartado 1.a del artículo 18 o al apartado 1.a) del artículo 20, cuando a dicha proposición le hayan seguido actos material conducentes a dicho encuentro[172].

2.4.10. Directiva 2016/680 del Parlamento Europeo y del Consejo de Europa, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales y la libre circulación de dichos datos, 2016

El 27 de abril de 2016, el Parlamento Europeo y el Consejo de la Unión Europea reconocieron y reafirmaron la importancia del adecuado tratamiento de los datos personales, resaltando su utilidad en la prevención, investigación, procesamiento y enjuiciamiento de actos delictivos. Debo destacar cómo se define la violación de la seguridad de los datos personales, así como uno de los principios relativos al tratamiento, dada su estrecha relación con los ciberdelitos cometidos contra la seguridad informática:

> Art. 3. A efectos de la presente Directiva se entenderá por [...] "violación de la seguridad de los datos personales": toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita, o la comunicación o acceso no autorizados a datos personales transmitidos, conservados o tratados de otra forma.

172 Perú, en el 2013, incorporaría este tipo penal a la legislación interna (art. 5 LDI). Sin embargo, la redacción no exige de "actos materiales conducentes a dicho encuentro", es decir, sanciona la mera propuesta o proposición.

> Art. 4. 1. Los Estados miembros dispondrán que los datos personales sean: [...] f) tratados de tal manera que garanticen una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidentales, mediante la aplicación de medidas técnicas y organizativas adecuadas.

2.4.11. Segundo Protocolo adicional al Convenio sobre la Ciberdelincuencia, relativo a la cooperación reforzada y la divulgación de prueba electrónica, 2022

El 12 de mayo de 2022, en Estrasburgo se adoptó el Segundo Protocolo adicional al Convenio sobre la Ciberdelincuencia con el objetivo de complementarlo y fortalecer las investigaciones/procesos relativos a la cibercriminalidad y el aseguramiento de la prueba digital[173].

Entre otras medidas, se adoptaron **(i)** procedimientos para mejorar la cooperación directa con proveedores y entidades de otros países[174], **(ii)** procedimientos para mejorar la cooperación internacional entre autoridades para la divulgación de datos informáticos almacenados[175], **(iii)** procedimientos relativos a la asistencia mutua en caso de emergencia[176] y **(iv)** procedimientos relativos a la cooperación internacional en ausencia de acuerdos internacionales aplicables[177].

---

173 Es importante resaltar que una delegación peruana estuvo presente en la ceremonia de apertura de la firma de este protocolo adicional.

174 Segundo Protocolo adicional al Convenio sobre la Ciberdelincuencia, art. 6.- Solicitud de información sobre el registro de nombres de dominio; y, art. 7.- Divulgación de información de los abonados.

175 Segundo Protocolo adicional al Convenio sobre la Ciberdelincuencia, art. 8.- Dar efecto a las órdenes de otra parte para la producción acelerada de información sobre los abonados y datos de tráfico; y, art. 9.- Divulgación acelerada de datos informáticos almacenados en caso de emergencia.

176 Segundo Protocolo adicional al Convenio sobre la Ciberdelincuencia, art. 10.- Asistencia mutua en caso de emergencia.

177 Segundo Protocolo adicional al Convenio sobre la Ciberdelincuencia, art. 11.- *Videoconferencia*, art. 12.- *Equipos conjuntos de investigación e investigaciones conjuntas.*

2.5. SISTEMA INTERAMERICANO

2.5.1. Segunda Reunión de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas sobre Delito Cibernético, 1999

Entre el 1 y el 3 de diciembre de 1997, se celebró la I Reunión de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas -en adelante, REMJA[178]-. En este encuentro se enumeraron los delitos que generaban preocupación para los Estados miembros, entre los cuales no se encontraba la delincuencia informática. No obstante, se resaltó la importancia de la cooperación internacional como una de sus conclusiones:

> 5. La cooperación legal internacional es esencial para el desarrollo de los sistemas de justicia en los países miembros de la OEA. En consecuencia, de conformidad con la legislación de cada país, es necesario trabajar, entre otras acciones, en la promoción de la Asistencia Jurídica Mutua, efectiva y ágil, particularmente en lo que se refiere a las extradiciones, en la solicitud de entrega de documentos y otros medios de prueba, en el establecimiento de canales seguros y rápidos de comunicación como los de Interpol, así como en el fortalecimiento del papel de las Autoridades Centrales[179].

178 La importancia de estas reuniones ha sido resaltada en los siguientes términos: "El proceso de las REMJA se ha constituido como uno de los foros políticos y técnicos de mayor importancia a nivel hemisférico en temas relacionados con el fortalecimiento y acceso a la justicia y la cooperación jurídica internacional en áreas relacionadas con la asistencia mutua en materia penal; extradición; políticas penitenciarias y carcelarias; delito cibernético; ciencias forenses; entre otras. El proceso de las REMJA ayuda a consolidar y fortalecer la cooperación jurídica y judicial a nivel regional" (Velasco San Martín, Cristos. *La jurisdicción y competencia sobre delitos cometidos a través de sistemas de cómputo e internet.* Valencia: Tirant lo Blanch, 2012, p. 184).

179 Organización de los Estados Americanos. *Conclusiones y recomendaciones (Adoptadas en la quinta sesión de trabajo celebrada el 3 de diciembre de 1997).* Reunión de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas. 1 al 3 de diciembre de 1997. Buenos Aires, 1997, p. 2. https://www.oas.org/juridico/spanish/remjai_recomend.pdf

Dos años después, entre el 1 y 3 de marzo de 1999, en Lima, se celebró la II REMJA[180]. En el diálogo de jefes de delegación se discutió el tema "Modernización y Fortalecimiento de los Sistemas de Justicia en las Américas: Intercambio de Experiencias, Nuevos Desarrollos y Cursos de Acción a Nivel Nacional e Internacional". La jefa de la delegación de los Estados Unidos de América trajo a colación -por primera vez- la delincuencia informática:

> En primer lugar, hizo mención a los delitos informáticos o cibernéticos y destacó la importancia de abordar este tema. Señaló que la informática no conoce de fronteras y puede atentar contra el derecho a la privacidad. Recomendó la formación de un grupo de trabajo que se ocupe del tema y que comparta información sobre el mismo[181].

Sobre la delincuencia informática, se arribó a la siguiente conclusión y recomendación:

> En vista de la importancia y la dificultad de las cuestiones que plantea el delito cibernético y la difusión y magnitud potencial de los problemas que presenta para nuestros países, recomendó el establecimiento de un grupo de expertos gubernamentales en el marco de la OEA con el siguiente mandato:
>
> 1. Hacer un diagnóstico de la actividad delictiva vinculada a las computadoras y la información, o que utiliza las computadoras como medio para cometer un delito;
> 2. Hacer un diagnóstico de la legislación, las políticas y las prácticas nacionales con respecto a dicha actividad;
> 3. Identificar las entidades nacionales e internacionales que tienen experiencia en la materia;
> 4. Identificar mecanismos de cooperación dentro del sistema interamericano para combatir el delito cibernético[182].

180 La ministra de Justicia María Carlota Valenzuela de Puelles participó en representación del Perú.

181 Organización de los Estados Americanos. *Informe Final de la Segunda Reunión de Ministros de Justicia o de Ministros Procuradores Generales de las Américas*. 1999, p. 11. https://www.oas.org/juridico/spanish/remjaii_inf_final.pdf

182 Ibid., p. 21.

2.5.2. Tercera Reunión de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas sobre Delito Cibernético, 2000

Entre el 1 y el 3 de marzo de 2000, en San José se llevó a cabo la III REMJA. En aquella oportunidad, el grupo de expertos[183] definió el delito cibernético de la siguiente forma: "Una actividad delictiva cuyo objetivo material o instrumental de comisión consiste en sistemas de tecnología de la información (incluidos, entre otros, los sistemas de telecomunicaciones e informática)"[184].

Entre las conclusiones y recomendaciones en torno a los denominados delitos cibernéticos, se encuentran las siguientes:

1.1 Establezcan una entidad o entidades públicas con la autoridad y función específica para llevar adelante la investigación y persecución del delito cibernético.

1.2 Emprendan las acciones necesarias para implementar legislación sobre delito cibernético, si aún no cuentan con la misma.

1.3 Realicen todos los esfuerzos necesarios para armonizar sus legislaciones en materia de delito cibernético, a fin de facilitar la cooperación internacional para la prevención y combate de estas actividades ilícitas.

1.4 Identifiquen sus necesidades de capacitación en materia de delito cibernético, propiciando esquemas de cooperación bilateral, regional y multilateral en este campo.

---

183 Sugiero revisar las recomendaciones brindadas por el Grupo de Trabajo en Materia de Delito Cibernético -cuya décima y última reunión se realizó en Washington D.C., el 28 y 29 de abril de 2022-. La misión de este grupo se describe en los siguientes términos: "Los delitos cibernéticos resaltan desafíos únicos debido a su carácter transnacional, y complejidad. En ese sentido la REMJA estableció un grupo de trabajo que se ocupa de manera específica en promover la cooperación jurídica hemisférica en la materia". De otro lado, reconocen tres objetivos: (1) Facilitar el intercambio de información y de experiencias, (2) Fortalecer la cooperación entre las autoridades especializadas en estos delitos y (3) Capacitar a jueces y fiscales de las Américas en el manejo de evidencia electrónica y en la investigación y juzgamiento de estos delitos. Se recomienda ver: https://www.oas.org/es/sla/dlc/cyber-es/grupo-trabajo.asp

184 Organización de los Estados Americanos. *Informe Final de la Tercera Reunión de Ministros de Justicia o de Ministros Procuradores Generales de las Américas.* 2000, p. 15. https://www.oas.org/consejo/sp/grupostrabajo/docs/mj00177s04.doc

1.5 Consideren la posibilidad de sumarse a mecanismos de cooperación o intercambio de información ya existentes, tales como el "Grupo de contacto de 24 horas/7 días", a fin de iniciar o recibir información.

1.6 Tomen medidas para sensibilizar al público, incluyendo a los usuarios del sistema educativo, del sistema legal y administración de justicia sobre la necesidad de prevenir y combatir el delito cibernético.

1.7 Consideren diversas medidas, incluyendo el establecimiento de un Fondo Específico Voluntario, para apoyar el desarrollo de la cooperación en el hemisferio sobre la materia.

1.8 Promuevan, en el marco de la OEA, el intercambio de información en materia de delito cibernético y la difusión de información sobre las actividades desarrolladas en esta materia, incluyendo la página web de la OEA[185].

Como se puede apreciar, a inicios del siglo XXI ya existía una llamado a la creación de unidades especiales de investigación dada la alta especialidad exigida para la identificación de los ciberdelincuentes. En el Perú se crearía la DIVINDAT en el 2005, mientras que la unidad de fiscales especializados en cibercriminalidad se conformaría casi dos décadas después.

2.5.3. Cuarta Reunión de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas sobre Delito Cibernético, 2002

La IV REMJA[186] se realizó en Trinidad y Tobago, entre el 10 y el 13 de marzo de 2002. En ella se recomendó que los Estados respondan el cuestionario elaborado por la Secretaría General de la OEA con el fin de evaluar los avances e implementación de las recomendaciones formuladas sobre la lucha contra la ciberdelincuencia. En esta ocasión, el Sr. Fernando Carrillo-Flores, representante del Banco Interamericano de Desarrollo, resaltó el apoyo que su institución brinda en el mejoramiento de la administración de justicia en las Américas[187]. Finalmente, se destacó la importancia de elaborar instrumentos jurídicos inte-

185 Ibid., pp. 27 y s.

186 El ministro de Justicia Fernando Olivera Vega participó en representación del Perú.

187 Organización de los Estados Americanos. *Informe Final de la Cuarta Reunión de Ministros de Justicia o de Ministros Procuradores Generales de las Américas*. 2002, p. 30. https://www.oas.org/juridico/spanish/remjaiv_inf_final.pdf

ramericanos con la finalidad de fortalecer la cooperación internacional. Entre las conclusiones y recomendaciones se tiene:

> 2. [...] b) Considerar la elaboración de los instrumentos jurídicos interamericanos pertinentes y de legislación modelo con el fin de fortalecer la cooperación hemisférica en el combate contra el delito cibernético, considerando normas relativas a la privacidad, la protección de la información, los aspectos procesales y la prevención del delito[188].

2.5.4. Quinta Reunión de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas sobre Delito Cibernético, 2004

En la V REMJA[189], celebrada en Washington D. C. entre el 28 y el 30 de abril de 2004, se resaltaron los resultados de la Reunión Inicial del Grupo de Expertos Gubernamentales en Materia de Delito Cibernético, llevada a cabo en la sede de la OEA, el 23 y 24 de junio de 2003. Es importante señalar que la Delegación de Brasil abordó la cooperación hemisférica en el establecimiento de mecanismos ágiles en el combate contra los delitos cibernéticos[190].

En esta reunión, se destacó la necesidad de la capacitación de los operadores jurídicos, la adopción de tipificaciones similares en la materia y la necesidad de que los estados se adhieran al Convenio de Budapest:

> 4. Que se dispense la capacitación internacional en relación con el delito cibernético a los Estados de la OEA que la soliciten, y que los Estados de la OEA en general consideren la posibilidad de asignar recursos que garanticen el suministro de esa capacitación [...].
>
> [...]
>
> 7. Que, en la medida de lo posible, los Estados miembros dispongan lo necesario para que las diferencias en la descripción de los delitos no vayan en detrimento de la eficiencia de la cooperación a través de la asistencia jurídica y judicial mutua y la extradición [...].

188 *Ibid.*, p. 35.

189 El ministro de Justicia Baldo Kresalja Roselló participó en representación del Perú.

190 Organización de los Estados Americanos. *Informe Final de la Quinta Reunión de Ministros de Justicia o de Ministros Procuradores Generales de las Américas*. 2004, p. 32. https://www.oas.org/juridico/spanish/remjaV_inf_final.pdf

8. Que los Estados miembro evalúen la conveniencia de la aplicación de los principios de la Convención del Consejo de Europa sobre la Delincuencia Cibernética (2001) y que consideren la posibilidad de adherirse a dicha Convención[191].

2.5.5. Estrategia Interamericana Integral para combatir las Amenazas a la Seguridad Cibernética: un enfoque multidimensional y multidisciplinario para la creación de una cultura de seguridad cibernética, 2004

El 8 de junio de 2004, los Estados Miembros de la OEA reconocieron "la urgente necesidad de incrementar la seguridad de las redes y sistemas de información comúnmente denominados Internet, a fin de abordar las vulnerabilidades y proteger a los usuarios, la seguridad nacional y las infraestructuras esenciales frente a las graves y perjudiciales amenazas que representan aquellos que podrían llevar a cabo ataques en el espacio cibernético con fines maliciosos o delictivos". En esta línea, resolvieron adoptar el proyecto de Estrategia Interamericana Integral de Seguridad Cibernética, instar su implementación, así como también sugerir que los Estados Miembros establezcan grupos nacionales de vigilancia y alerta también denominados *Equipos de Respuesta de Seguridad en Computadoras* (CSIRT).

Además, los Estados Miembros de la OEA resaltaron la importancia de las TIC en el crecimiento de la economía mundial, así como en la necesidad de aumentar la conectividad en las Américas. No obstante, también reconocieron que puede ser utilizada para malversar y manipular, así como invadir la privacidad de los usuarios y estafar a los negocios e, incluso, causar daños severos al afectar redes de electricidad, aeropuertos o suministros de agua.

Tomando como base los esfuerzos y conocimientos especializados del Comité Interamericano contra el Terrorismo (CICTE), la Comisión Interamericana de Telecomunicaciones (CITEL) y la Reunión de Ministros de Justicia o Ministros o Procuradores Generales de las Américas (REMJA), se propusieron las siguientes conclusiones como parte de la Estrategia Interamericana Integral de Seguridad Cibernética:

191 *Ibid.*, p. 43.

1. Coordinación y cooperación permanente entre las Secretarías del CICTE, la CITEL y el Grupo de Expertos Gubernamentales en Materia de Delito Cibernético de la REMJA.
2. Fortalecimiento de la coordinación entre las autoridades y entidades nacionales, incluidos los CSIRT nacionales, que trabajan en cuestiones relacionadas con la seguridad cibernética.
3. Establecimiento de un sitio web conjunto en el que pueda introducirse la información pertinente sobre seguridad cibernética generada por el CICTE, la CITEL y el Grupo de Expertos Gubernamentales en Materia de Delito Cibernético de la REMJA, a fin de permitir un fecundo intercambio de ideas y facilitar el intercambio de información.
4. Los Estados miembros deberán llevar a cabo, junto con el CICTE, la CITEL y el Grupo de Expertos Gubernamentales de la REMJA en materia de Delito Cibernético, un programa interamericano de concientización del público acerca de la seguridad y la ética cibernéticas en el que se destaquen [los siguientes aspectos]: las ventajas y responsabilidades del uso de redes de información; las mejores prácticas de seguridad y protección; las posibles consecuencias negativas del uso indebido de las redes; cómo reportar un incidente cibernético y a quién; e información técnica y práctica relacionada con la seguridad cibernética.
5. Exámenes periódicos de las iniciativas y programas en materia de seguridad cibernética del CICTE, la CITEL y el Grupo de Expertos Gubernamentales de la REMJA en Materia de Delito Cibernético, y sobre la implementación de la Estrategia, que realizarán estos tres órganos, con un informe conjunto de progreso para la Asamblea General.

2.5.6. Sexta Reunión de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas sobre Delito Cibernético, 2006

En Santo Domingo, entre el 24 y el 26 de abril de 2006, se celebró la VI REMJA[192], en la que intervino el Director General de Asuntos Jurídicos

192 Mediante Resolución Ministerial N.° 151-2006-JUS del 19 de abril de 2006 se autorizó el viaje del abogado Edgardo Hopkins Torres, Jefe del Gabinete de Asesores de la Asesoría Técnica del Ministerio de Justicia para que participe en la VI REMJA.

del Consejo de Europa, quien se refirió a la cooperación entre la OEA y dicho organismo. En esta línea, se enfatizó los resultados emanados de la Conferencia denominada "La cibercriminalidad: Un desafío global, una respuesta universal" organizada por el Consejo de Europa y el Ministerio de Justicia del Reino de España en coordinación con la OEA[193].

Se recomendó nuevamente a los Estados miembros a adherirse al Convenio de Budapest, así como fortalecer el intercambio de información -esencial en la investigación de este tipo de delitos-:

> 3. Que, teniendo en cuenta las recomendaciones adoptadas por el Grupo de Expertos Gubernamentales y por la REMJA-V y los avances alcanzados entre esta y la presente reunión, se continúe fortaleciendo la cooperación con el Consejo de Europa con el fin de facilitar que los Estados Miembros de la OEA consideren la aplicación de los principios de la Convención del Consejo de Europa sobre la Delincuencia Cibernética y la adhesión a la misma, así como la adopción de las medidas legales y de otra naturaleza, que sean necesarias para su implementación. Asimismo, que se continúen fortaleciendo los mecanismos que permitan el intercambio de información y la cooperación con otras organizaciones e instancias internacionales en materia de delito cibernético, tales como las Naciones Unidas, la Unión Europea, el Foro de Cooperación Económica del Pacífico Asiático, la OCDE, el G-8, el "Commonwealth" e INTERPOL, de manera que los Estados miembros de la OEA puedan aprovechar los desarrollos dados en dichos ámbitos.
>
> 4. Que los Estados miembros creen unidades especializadas de investigación de los delitos cibernéticos, se identifiquen las autoridades que servirán como puntos de contacto sobre la materia y se agilice el intercambio de información y la obtención de pruebas. Asimismo, fomentar la cooperación en los esfuerzos para combatir los delitos cibernéticos entre las autoridades gubernamentales

193 Organización de los Estados Americanos. *Informe Final de la Sexta Reunión de Ministros de Justicia o de Ministros Procuradores Generales de las Américas*. 2006, p. 37.

y los proveedores de servicios de Internet y otras empresas del sector privado que presten servicio de transmisión de datos[194].

2.5.7. Séptima Reunión de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas sobre Delito Cibernético, 2008

Entre el 28 y el 30 de abril de 2008, en Washington D. C. se llevó a cabo la VII REMJA[195]. Al igual que en otras ocasiones, se instó a los Estados miembros a adherirse al Convenio de Budapest, pero también resaltó la necesidad de adoptar estrategias vinculadas a la seguridad cibernética:

> 4. Que las Secretarías del Comité Interamericano contra el Terrorismo (CICTE) y la Comisión Interamericana de Telecomunicaciones (CITEL) y el Grupo de Trabajo en Delito Cibernético de las REMJA continúen desarrollando las acciones de coordinación y cooperación permanentes para asegurar la implementación de la Estrategia Interamericana Integral de Seguridad Ciudadana adoptada mediante la resolución AG/RES. 2004 (XXXIV-O/04) de la Asamblea General de la OEA[196].

2.5.8. Octava Reunión de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas sobre Delito Cibernético, 2010

Del 24 al 26 de febrero de 2010, en Brasilia se celebró la VIII REMJA[197], en la que se recordó que los Estados deben responder las solicitudes que formule la Secretaría General de la OEA para completar o actualizar el *Portal Interamericano de cooperación en materia de Delito Cibernético*, alojado en la web de

---

194 Organización de los Estados Americanos. *Conclusiones y recomendaciones (Aprobadas en la quinta plenaria el 26 de abril de 2006 y revisada por la Comisión de Estilo en las sesiones celebradas los días 19 y 21 de julio y 3 de agosto de 2006).* 2006, p. 3.

195 La representante permanente de la misión permanente de Perú ante la OEA, María Zavala, participó en representación de nuestro país.

196 Organización de los Estados Americanos. *Conclusiones y recomendaciones de la REMJA VII.* 2008, p. 1. https://www.oas.org/juridico/spanish/cybVII_CR.pdf

197 El juez superior y presidente de la Cuarta Sala Penal Especial para Procesos Anticorrupción de la Corte Superior de Justicia del Perú, Ricardo Alberto Brousset Salas, participó en representación de nuestro país.

la OEA. Además, se destacaron los talleres organizados en esta materia y que fueron liderados por Estados Unidos:

> 4. Expresar su satisfacción por los resultados alcanzados en los talleres para fortalecer la capacidad de los Estados en el desarrollo de legislación y medidas procesales relacionadas con el delito cibernético y las pruebas electrónicas, los cuales fueron realizados, bajo el liderazgo de los Estados Unidos como Presidente del Grupo de Trabajo de las REMJA en Delito Cibernético y con el auspicio financiero de este Estado, el apoyo de los Estados en que se llevaron a cabo y la cooperación de la Secretaría General de la OEA, en Puerto España, Trinidad y Tobago; Bogotá, Colombia; Santiago, Chile; Ciudad de Panamá, Panamá; y Asunción, Paraguay[198].

Como se ha indicado líneas arriba, la capacitación de los operadores jurídicos es fundamental para comprender los alcances de este tipo de delitos y realizar investigaciones adecuadas.

2.5.9. Declaración de Río sobre el Delito Cibernético, 2012

El 23 de marzo de 2012, la Comisión Delegada de Ministros de Justicia y autoridades homólogas de la Conferencia de Ministros de Justicia de los Países Iberoamericanos decidió "respaldar los primeros pasos que se han dado en la línea de lucha contra la delincuencia organizada para iniciar el debate sobre la elaboración y firma de un documento internacional iberoamericano, capacidad de dar respuesta [...] e impulsar la modificación de las legislaciones penales de manera armonizada". Entre las líneas generales dictadas con la finalidad de concretar un borrador de Convenio Iberoamericano para regular el Ciberdelito tenemos:

> 2 La utilización "torcida" de estas nuevas tecnologías está poniendo en riesgo, y en no pocas ocasiones lesionando, tanto bienes jurídicos tradicionales (intimidad, patrimonio, propiedad intelectual,

198 Organización de los Estados Americanos. *Conclusiones y recomendaciones de la REMJA VIII.* 2010, pp. 7-8. https://www.oas.org/dil/esp/REMJA-VIII_doc_4-10_rev1_esp.doc

libertad sexual de las personas menores de edad) como nuevos intereses originados por el desarrollo tecnológico. Se trata de una nueva forma de delincuencia: la cibercriminalidad.

3 La cibercriminalidad hace referencia al fenómeno criminológico que engloba todas las formas de delincuencia surgidas con la revolución tecnológica de las últimas décadas, en las que las tecnologías de la información y la comunicación (TIC) son el instrumento de ejecución de la infracción penal.

4 Se entenderá como cibercrimen o ciberdelito cualquier delito llevado a cabo en el ciberespacio, que está universalizado y sujeto a una revolución tecnológica permanente y obliga a una revisión de los instrumento legislativos, judiciales y policiales pensados para los delitos cometidos en el espacio físico nacional tradicional.

2.5.10. Novena Reunión de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas sobre Delito Cibernético, 2012

En Quito, el 28 y 29 de noviembre de 2012, se realizó la IX REMJA[199]. Las recomendaciones fueron similares a las anteriores: Continuar fortaleciendo el intercambio de información y la cooperación con otras organizaciones internacionales en materia de delito cibernético; continuar fomentando las relaciones entre las autoridades responsables de la prevención, investigación y procesamiento de los delitos cibernéticos y el sector privado; reconocer los resultados de los talleres de capacitación realizados en Saint Jhon´s (Antigua y Barbuda), Bogotá (Colombia), Miami (Estados Unidos), Ciudad de Guatemala (Guatemala), Ciudad de México (México), Lima (Perú) y Montevideo (Uruguay).

Me parece relevante destacar que, si bien se recomendó, nuevamente, evaluar la adhesión de los Estados miembros al Convenio de Budapest, Brasil pidió evaluar los principios de dicha convención y analizar si son afines a la región latinoamericana.

199 Mediante Resolución de la Fiscalía de la Nación N.º 3109-2012-MP-FN del 23 de noviembre del 2012 se autorizó al Fiscal Supremo Carlos Ramos Heredia, Jefe de la Fiscalía Suprema de Control Interna del Ministerio Público a participar en la IX REMJA.

> Brasil opina que la Convención del Consejo de Europa sobre la Delincuencia Cibernética es fruto de un proceso de negociación regional cuyo resultado es adecuado para esa realidad. No obstante, Brasil considera que sería necesario revisar los principios de esa Convención para cubrir las necesidades de las Américas, ya que apoya soluciones basadas en un paradigma de gestión del espacio cibernético inclusivo, centrado en la persona y orientado al desarrollo[200].

Es importante tomar en cuenta que Brasil se adhirió al citado convenio nueve años después.

2.5.11. Convenio Iberoamericano de Cooperación sobre investigación, aseguramiento y obtención de prueba en materia de ciberdelincuencia, 2014

El 28 de mayo de 2014, los Estados miembros de la Conferencia de Ministros de Justicia de los Países Iberoamericanos (COMJIB) celebraron el Convenio Iberoamericano de Cooperación sobre Investigación, Aseguramiento y Obtención de Prueba en materia de Ciberdelincuencia. Este convenio busca reforzar la cooperación mutua de las partes para enfrentar el fenómeno delictivo bajo estudio, destacando el principio de cooperación mutua, el respeto de los derechos humanos en la solicitud o ejecución de actividades de cooperación, las medidas de aseguramiento, las diligencias de investigación, las autoridades centrales, las solicitudes de cooperación, el procedimiento para la tramitación de las solicitudes de cooperación, entre otros.

En materia sustantiva, es importante destacar el concepto de ciberdelincuencia acuñado:

> **Art. 2.** A efectos del presente Convenio: 1. Por ciberdelincuencia se entiende cualquier forma de criminalidad ejecutada en el ámbito social definido por el uso de las Tecnologías de la Información y Comunicación.

200 Organización de los Estados Americanos. *Conclusiones y recomendaciones de la REMJA IX*. 2012, p. 9, n. 1. https://cejamericas.org/wp-content/uploads/2019/12/REMJA_IX-1.pdf

2.5.12. Décima Reunión de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas sobre Delito Cibernético, 2015

En Bogotá, entre el 15 y el 16 de octubre de 2015, se realizó la X REMJA[201]. Se reconocieron las capacitaciones realizadas entre el 2012 y el 2015 en Ciudad de Guatemala (Guatemala), Montevideo (Uruguay), Miami (Estados Unidos), Lima (Perú), Asunción (Paraguay), Ciudad de Panamá (Panamá) y San Pablo (Brasil). En esta reunión, a diferencia de las previas, se dejó de utilizar la denominación *delitos cibernéticos* y se reemplazó por *delitos relacionados con computadoras y otros equipos electrónicos.*

Entre otras conclusiones y recomendaciones, se resaltó:

> 9. Que la Secretaría Técnica de las REMJA continúe dando difusión a los desarrollos dados en el marco de la OEA y por los Estados en materia de cooperación jurídica internacional sobre delitos relacionados con computadoras y otros equipos electrónicos, a través del "Boletín de Cooperación Jurídica" elaborado y distribuido electrónicamente por ella. Asimismo, invitar a los Estados a que contribuyan con información sobre los desarrollos que den en este campo para su difusión en dicho boletín[202].

2.5.13. Décima Primera Reunión de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas sobre Delito Cibernético, 2021

Siendo el anfitrión Ecuador, entre el 18 y 19 de mayo de 2021, se celebró virtualmente la XI REMJA[203]. Entre las conclusiones y recomendaciones, resaltan las siguientes:

> 5. Fortalecer, a través del Grupo de Trabajo de las REMJA, la cooperación internacional en cuatro aspectos: i) fortalecimiento de capacidades; ii) generación de evidencia sobre los ciberdelitos; iii)

201 El ministro de Justicia Gustavo Adrianzén participó en representación del Perú.

202 Organización de los Estados Americanos. *Conclusiones y recomendaciones de la REMJA X.* 2015, pp. 9-10. https://www.oas.org/es/sla/dlc/remja/pdf/remja_x_rec_conc_sp.pdf

203 El ministro de Justicia Eduardo Vega Luna participó en representación del Perú.

cooperación jurídica en materia de criminalidad cibernética; y iv) desarrollos legislativos.

6. Expresar su satisfacción por la organización de un foro virtual sobre la Adecuación de las Legislaciones a las Normas Internacionales contra los Delitos Cibernéticos, que tuvo lugar el 24 de agosto de 2020, el cual formó parte de una serie de sesiones virtuales organizadas por la Secretaría de Asuntos Jurídicos sobre el Derecho Interamericano en Tiempos de Pandemia, durante el cual los expertos subrayaron la importancia de la cooperación jurídica y discutieron las herramientas disponibles para combatir la ciberdelincuencia en el contexto de la pandemia en curso[204].

Como se puede apreciar, en el sistema interamericano se observan significativos esfuerzos de unión y cooperación internacional en la lucha contra la ciberdelincuencia. Las reuniones de ministros de justicia y las estrategias interamericanas son claros ejemplos de este compromiso. Es crucial destacar que la capacitación juega un papel fundamental en estos esfuerzos, lo cual se evidencia en el reciente taller organizado por la OEA en Lima, entre el 20 y el 22 agosto de este año: *Taller de la REMJA para fiscales sobre criptomonedas: siguiendo el dinero*[205].

2.6. SISTEMA DE NACIONES UNIDAS

A continuación, mencionaré los principales congresos organizados, así como las resoluciones emitidas por la Asamblea General de las Naciones Unidas, desde 1990, pues evidencian la importancia de las TIC en el desarrollo social, económico y político; pero también la preocupación internacional por su uso

204 Organización de los Estados Americanos. *Conclusiones y recomendaciones de la REMJA XI.* 2021, p. 10. https://www.oas.org/es/sla/dlc/remja/pdf/remja_xi_rec_conc_sp.pdf

205 En este taller se abordaron los siguientes tópicos: (1) Herramientas para investigar casos con criptomonedas, (2) Métodos usados para lavado de activos con criptomonedas, (3) Herramientas de cooperación internacional, (4) Experiencias sobre la investigación de ataques de *ransomware* contra cooperaciones y (6) Caso de estudio en la región. Los detalles pueden ser analizados en: https://www.oas.org/ext/es/principal/calendario/evento/id/446

indebido -advirtiéndose desde épocas tempranas, incluso, su conexión con el crimen organizado-.

2.6.1. VIII Congreso de las Naciones Unidas, sobre prevención del delito y tratamiento del delincuente, 1990[206]

Entre los temas abordados en las resoluciones aprobadas, se encuentran los *delitos relacionados con la informática*. Los estados reconocieron la importancia de los sistemas, ya que almacenan datos políticos, económicos, médicos, sociales y personales; advirtiendo que su manipulación podría amenazar la vida de las personas, los derechos humanos y las libertades fundamentales. Asimismo, se reconoció el aumento de casos de uso indebido de las técnicas informáticas como modalidad de delincuencia económica y la dificultad de detectar este tipo de ilícitos[207].

Es importante destacar que, en esta época, ya se advertían los vínculos que podían existir entre la criminalidad organizada y la delincuencia informática precisando que podría emplearse para el lavado de activos -entonces denominado *blanqueo de capitales*-. En cuanto a nuevas tendencias delictivas, se expresó la siguiente reflexión:

> 71. Con referencia a la delincuencia relacionada con la informática, se señaló que con el mayor empleo del proceso de datos en las economías y burocracias de los distintos países se había difundido la comisión de actos delictivos. La injerencia transnacional en los sistemas de proceso de datos de otros países había atraído la atención de todo el mundo. El problema principal de los delitos informáticos radicaba en la reproducción y la difusión no autorizada de programas informáticos y en el uso indebido de los cajeros automáticos. Aunque hasta el momento otras formas de delitos informáticos no estaban tan difundidas, era preciso adop-

206 El VIII Congreso se llevó a cabo en La Habana, Cuba, entre el 27 de agosto y el 7 de setiembre de 1990.

207 *Octavo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente*. La Habana, 27 de agosto a 7 de setiembre de 1990. https://www.unodc.org/documents/congress/Previous_Congresses/8th_Congress_1990/028_ACONF.144.28.Rev.1_Report_Eighth_United_Nations_Congress_on_the_Prevention_of_Crime_and_the_Treatment_of_Offenders_S.pdf

> tar medidas preventivas para evitar su aumento. En general se suponía que había un gran número de casos de delitos informáticos no registrados. En vista de que los delitos informáticos eran un fenómeno relativamente nuevo, y debido a la ausencia de medidas que pudieran contrarrestarlo, el uso deshonesto de las computadoras podría tener consecuencias desastrosas. A este respecto, se recomendó que se establecieran normas y directrices sobre la seguridad de las computadoras a fin de ayudar a la comunidad internacional a hacer frente a estas formas de delincuencia. Con todo, se subrayó que el problema de los delitos informáticos no debía ser motivo para que se desalentara el apoyo a las medidas internacionales encaminadas a fomentar el uso de la informática en los sistemas de justicia penal[208].

2.6.2. X Congreso de las Naciones Unidas, sobre prevención del delito y tratamiento del delincuente. La delincuencia y la justicia frente a los retos del siglo XXI, 2000[209]

La Asamblea General, en su resolución 53/110, hizo suyo el programa de trabajo del Congreso, incluida la celebración de cuatro cursos prácticos de carácter técnico sobre los siguientes temas: (a) lucha contra la corrupción, (b) delitos relacionados con la red informática, (c) participación de la comunidad en la prevención de la delincuencia y (d) la mujer en el sistema de justicia penal. El curso práctico estuvo a cargo de 17 expertos en la materia[210]. Asimismo, fue organizado por el Instituto de Asia y el Lejano Oriente para la Prevención del

208 *Octavo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente*, cit., p. 230, parágrafo 71.

209 *Informe del Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente*. Viena, 10 al 17 de abril de 2000. https://www.unodc.org/documents/congress/Previous_Congresses/10th_Congress_2000/030_ACONF.187.15_Report_of_the_Tenth_United_Nations_Congress_on_the_Prevention_of_Crime_and_the_Treatment_of_Offenders_S.pdf

210 Los expertos que participaron fueron: L.C. Amarnathan (India), Cormac Callanan (Irlanda), Peter N. Grabosky (Australia), Masahito Inouye (Japón), Nigel Jones (Reino Unido de Gran Bretaña e Irlanda del Norte), Ekkehart Kappler (Alemania), Henrik W.K. Kaspersen (Países Bajos), Margo L. Langford (Canadá), Victor Lo (Región Administrativa Especial de China), Keith Mitchell (Reino Unido de Gran Bretaña e Irlanda del Norte), Hans G. Nilsson (Consejo de la Unión Europea), Donald K. Piragoff (Canadá), Mary Riley (Estados Unidos de América), Gregory P. Schaffer (Esta-

Delito y el Tratamiento del Delincuente y se celebró el 15 de abril. Se adoptó la expresión *delito informático* para "referirse tanto a las formas completamente nuevas de delincuencia relacionadas con las computadoras, las redes y sus usuarios, como a las formas de delitos más tradicionales que ahora se cometían con el uso o la ayuda de equipo informático"[211]. Entre otros temas, se discutió la importancia de la promulgación de leyes penales adecuadas para la lucha contra este fenómeno delictivo, la necesidad de comprender que los bienes tradicionales no se asimilan a los datos informáticos -destacando su naturaleza incorpórea- y los problemas jurídicos relacionados a su recopilación, conservación y utilización en los procesos judiciales. Es más, se discutió la necesidad y rigurosidad que se debía exigir al diferenciar la interceptación de datos en la fase de transmisión y la búsqueda de datos almacenados. Finalmente, hubo acuerdo general en que "los Estados debían tratar de armonizar, cuando procediera, las disposiciones pertinentes sobre tipificación de delitos, pruebas y procedimientos"[212].

Se llegó a las siguientes conclusiones:

a) los delitos informáticos debían tipificarse;
b) se requerían leyes procesales adecuadas para la investigación y el enjuiciamiento de los delincuentes en el ámbito cibernético;
c) el Gobierno y la industria debían aunar esfuerzos en pos del objetivo común de prevenir y combatir los delitos informáticos a fin de velar por que la Internet fuese un lugar seguro;
d) se necesitaba una mayor cooperación internacional para rastrear a los delincuentes en la Internet;
e) las Naciones Unidas debían adoptar nuevas medidas con respecto a la prestación de cooperación y asistencia técnica en la esfera de la delincuencia relacionada con las redes informáticas[213].

---

dos Unidos de América), Ulrich Sieber (Alemania), Vittorio Stanca (Italia). Michael Sussman (Estados Unidos de América).

211 *Informe del Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente*, cit., p. 29, parágrafo 165.

212 *Informe del Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente*, cit., p. 30, parágrafo 173.

213 *Informe del Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente*, cit., p. 31, parágrafo 174.

2.6.3. Resolución 55/63, sobre la lucha contra la utilización de la tecnología de la información con fines delictivos, 2000[214]

En la octogésima primera sesión plenaria, la Asamblea General aprobó el tema 105 del programa, el cual giró en torno al uso de las TIC con fines ilícitos. En ella se recordó que, en la Declaración del Milenio, los Estados Miembros acordaron velar porque los beneficios de las nuevas tecnologías alcancen a todos los ciudadanos; sin embargo, también se expresó la preocupación por cuanto los avances informáticos abrieron nuevas posibilidades de actividades delictivas. Así, se adoptaron los siguientes compromisos:

a) los Estados deben velar para que en su legislación y en la práctica se eliminen los refugios seguros para quienes utilicen la tecnología de la información con fines delictivos;
b) debe coordinarse entre todos los Estados interesados la cooperación en lo que se refiere a la vigilancia del cumplimiento de la ley y la investigación y el enjuiciamiento de los casos en que se utilice la tecnología de la información con fines delictivos en el plano internacional;
c) los Estados deben intercambiar información acerca de los problemas a que hacen frente en la lucha contra la utilización de la tecnología de la información con fines delictivos;
d) el personal encargado de hacer cumplir la ley debe contar con capacitación y equipo adecuado para hacer frente a la utilización de la tecnología de la información con fines delictivos;
e) los sistemas jurídicos deben proteger el carácter confidencial, la integridad y la disponibilidad de datos y sistemas respecto a la injerencia no autorizada y hacer que los abusos graves se tipifiquen como delito;
f) los sistemas jurídicos deben permitir la conservación de datos electrónicos relativos a investigaciones criminales concretas, y un rápido acceso a esos datos;
g) los regímenes de asistencia mutua deben velar por la investigación oportuna de la utilización de la tecnología de la información con

214 La Resolución fue emitida el 4 de diciembre de 2000.

fines delictivos y la reunión y el intercambio oportunos de pruebas en esos casos;

h) debe sensibilizarse al público en general acerca de la necesidad de prevenir y combatir la utilización de la tecnología de la información con fines delictivos;

i) en la medida de lo posible, la tecnología de la información deberá diseñarse de forma que facilite la prevención y detección de su utilización con fines delictivos, la localización de los delincuentes y la reunión de pruebas;

j) la lucha contra la utilización de la tecnología de la información con fines delictivos requiere la elaboración de soluciones que tengan en cuenta tanto la protección de las libertades individuales y el derecho a la intimidad como la preservación de la capacidad de los gobiernos para combatir esa utilización con fines delictivos.

2.6.4. Resolución 56/121, sobre la lucha contra la utilización de la tecnología de la información con fines delictivos, 2001[215]

En la octogésima octava sesión plenaria, la Asamblea General resaltó la labor de organizaciones internacionales y regionales, en particular, el trabajo realizado por el Consejo de Europa en la preparación del Convenio sobre la Ciberdelincuencia. Además, se resaltó el diálogo entre los gobiernos y el sector privado en lo que a seguridad y confianza en el ciberespacio se refiere. Al finalizar la sesión, se acordó:

1. Invita a los Estados miembros a que, al elaborar leyes y políticas nacionales y al adoptar prácticas para luchar contra la utilización de la tecnología de la información con fines delictivos, tengan en cuenta, según proceda, la labor y los logros de la Comisión de Prevención del Delito y Justicia Penal y de otras organizaciones internacionales y regionales.
2. Toma nota del valor de las medidas enunciadas en su resolución 55/63, e invita nuevamente a los Estados miembros a que las tengan en cuenta en su lucha contra la utilización de la tecnología de la información con fines delictivos.

215 La Resolución fue emitida el 19 de diciembre de 2001.

3. Decide aplazar el examen de este tema, mientras se realiza la labor prevista en el plan de acción contra los delitos de alta tecnología y relacionados con las redes informáticas de la Comisión de Prevención del Delito y Justicia Penal.

2.6.5. Resolución 64/211, sobre la creación de una cultura mundial de seguridad cibernética y balance de las medidas nacionales para proteger las infraestructuras de información esenciales, 2009[216]

En la sexagésima sexta sesión plenaria, la Asamblea General reconoció que cada país miembro debe determinar sus propias infraestructuras de información esencial, pero, al mismo tiempo, expresó su preocupación "porque las amenazas para el funcionamiento fiable de las infraestructuras de información esenciales y la integridad de la información transmitida por esas redes están aumentando en complejidad y gravedad y afectando el bienestar interno, nacional e internacional". Por este motivo:

1. Invita a los Estados miembros a utilizar, siempre y cuando lo consideren procedente, el instrumento de autoevaluación voluntaria de las medidas nacionales para proteger las infraestructuras de información esenciales que figura en el anexo a fin de contribuir a la evaluación de sus esfuerzos en ese sentido y fortalecer su seguridad cibernética de manera que se resalten los ámbitos en que se necesiten medidas adicionales con el objetivo de ampliar la cultura mundial de seguridad cibernética.
2. Alienta a los Estados miembros y a las organizaciones regionales e internacionales pertinentes que hayan elaborado estrategias de seguridad cibernética y de protección de las infraestructuras de información esenciales a que compartan las mejores prácticas y las medidas que puedan ayudar a otros Estados miembros en sus esfuerzos por facilitar el logro de la seguridad cibernética proporcionando esa información al secretario general para que la recopile y la difunda entre los Estados miembros.

El anexo al que se hace referencia aborda los siguientes tópicos: (i) balance de las necesidades y estrategias en materia de seguridad cibernética, (ii) funciones

216 La Resolución fue emitida el 21 de diciembre de 2009.

y responsabilidades de los interesados, (iii) procesos políticos y participación, (iv) cooperación entre el sector público y privado, (v) gestión de incidentes y recuperación, (vi) marcos jurídicos y (vii) creación de una cultura mundial de seguridad cibernética.

2.6.6. XII Congreso de las Naciones Unidas sobre Estrategias amplias ante problemas globales: Los sistemas de prevención del delito y justicia penal y su desarrollo en un mundo en evolución, 2010[217]

En la Declaración de Salvador —en torno a las estrategias amplias ante problemas globales: los sistemas de prevención del delito y justicia penal y su desarrollo en un mundo en evolución—, los Estados miembros de las Naciones Unidas manifestaron lo siguiente:

> 39. Observamos que el desarrollo de las tecnologías de la información y las comunicaciones y el uso cada vez más frecuente de internet crean nuevas oportunidades para los delincuentes y facilitan la proliferación de la delincuencia.
>
> 40. Recomendamos la vulnerabilidad de los niños, y exhortamos al sector privado a que promueva y apoye las iniciativas para prevenir el abuso sexual de los niños y su explotación en internet.
>
> 41. Recomendamos a la Oficina de las Naciones Unidas contra la Droga y el Delito que, en cooperación con los Estados miembros, las organizaciones internacionales pertinentes y el sector privado, preste asistencia técnica a los Estados que lo soliciten y les imparta capacitación para mejorar su legislación nacional y reforzar la capacidad de las autoridades nacionales, a fin de que hagan frente a los delitos cibernéticos, incluso mediante la prevención, la detección, la investigación y el enjuiciamiento de esos delitos en todas sus formas, y para aumentar la seguridad de las redes informáticas.
>
> 42. Invitamos a la Comisión de Prevención del Delito y Justicia Penal a que estudie la posibilidad de convocar a un grupo intergubernamental de expertos de composición abierta para que realice un estudio exhaustivo del problema del delito cibernético y las

217 El XII Congreso se llevó a cabo en Salvador, Brasil, entre el 12 y el 19 de abril de 2010.

> respuestas de los Estados miembros, la comunidad internacional y el sector privado ante este fenómeno, incluido el intercambio de información sobre legislación nacional, mejores prácticas, asistencia técnica y cooperación internacional, con miras a examinar opciones para fortalecer las actuales respuestas jurídicas o de otra índole ante el delito cibernético en los planos nacional e internacional y proponer otras nuevas.

Durante el debate previo se reconocieron que los adelantos tecnológicos posibilitan nuevas modalidades de delitos tradicionales -como el fraude y la distribución de material de abuso sexual infantil- y conciben otros nuevos -como el envío de spam, la penetración en redes informáticas, el *phishing*, la piratería digital, la propagación maliciosa de virus, así como ataques contra infraestructuras de información esenciales. Asimismo, se resaltó que las organizaciones terroristas emplean las TIC, ya que facilitan sus actividades. Además, se subrayó que la rápida evolución de las TIC rezaga las legislaciones locales a lo que se suma la insuficiente cooperación internacional. Un punto importante -que, a la fecha, no hemos solucionado- fue el reconocimiento de que los países en desarrollo eran los más vulnerables a este nuevo tipo de delitos.

2.6.7. XIII Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, 2015[218]

En el décimo tercer congreso se aprobó la Declaración de Doha sobre la Integración de la Prevención del Delito y la Justicia Penal en el Marco Más Amplio del Programa de las Naciones Unidas para Abordar los Problemas Sociales y Económicos y Promover el Estado de Derecho a Nivel Nacional e Internacional y la Participación Pública. Entre las declaraciones que se acordaron, resalto las relacionadas al uso de las TIC en la comisión de delitos:

> 9. Procuramos garantizar que los beneficios de los avances económicos, sociales y tecnológicos se conviertan en un factor positivo que dinamice nuestra labor para prevenir y combatir las formas nuevas y emergentes de delincuencia. Reconocemos nuestra responsabilidad de afrontar correctamente las nuevas y cambiantes amenazas que plantean estos delitos. Así pues, nos esforzamos por:

218 El XIII Congreso se llevó a cabo en Doha, Catar, entre el 12 y el 19 de abril de 2015.

[...]

b) Estudiar medidas concretas destinadas a crear un entorno cibernético seguro y resistente, prevenir y combatir las actividades delictivas realizadas por internet, prestando especial atención a la detección del robo, [denunciar] la captación de personas con fines de trata y [promover] la protección de los niños contra la explotación y los abusos a través de internet. [Asimismo,] reforzar la cooperación entre los organismos de aplicación de la ley en los planos nacional e internacional, incluso para identificar y proteger a las víctimas, entre otras cosas, eliminando de internet todo contenido pornográfico en el que aparezcan menores, en particular imágenes de abusos sexuales contra niños. [También,] aumentar la seguridad de las redes informáticas y proteger la integridad de la infraestructura correspondiente, y procurar prestar asistencia técnica a largo plazo y crear capacidad a fin de que las autoridades nacionales puedan combatir con más eficacia la delincuencia cibernética, incluso mediante la prevención, la detección, la investigación y el enjuiciamiento de estos delitos en todas sus formas. Además, tomamos conocimiento de las actividades del grupo intergubernamental de expertos de composición abierta encargado de realizar un estudio exhaustivo del problema del delito cibernético y las respuestas de los Estados miembros, la comunidad internacional y el sector privado ante ese fenómeno, e invitamos a la Comisión de Prevención del Delito y Justicia Penal a que estudie la posibilidad de recomendar que el grupo de expertos, basándose en su propia labor, siga intercambiando información sobre legislación nacional, mejores prácticas, asistencia técnica y cooperación internacional, con miras a examinar opciones para fortalecer las actuales respuestas y proponer nuevas respuestas jurídicas o de otra índole frente al delito cibernético a nivel nacional e internacional.

En las diversas mesas de debate se destacó la relación entre la ciberdelincuencia y el tráfico de bienes culturales -delito emergente-, así como su conexión con el crimen organizado y la corrupción. En la misma línea, se resaltó que los grupos delictivos organizados estaban haciendo amplio uso del ciberespacio, con lo que contribuían a la naturaleza transnacional del delito cibernético. Además, se señaló que los delincuentes ya no necesitaban contar con conocimientos especializados y que la pobreza podía condicionar a los jóvenes a unirse a grupos delictivos organizados.

2.6.8. Informe de la Reunión del Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético, 2020[219]

El 29 de julio del 2020, en la sexta sesión celebrada, el grupo de expertos aprobó el informe que recogía conclusiones y recomendaciones preliminares que se presentarían a la Comisión de Prevención del Delito y Justicia Penal. Este documento aborda dos grandes campos: Cooperación Internacional y Prevención. De la primera área, destaco los siguientes típicos:

> a) En cuanto al alcance de la definición de "delito cibernético" a efectos de cooperación internacional, los países debería tipificar como delito los actos de ciberdelincuencia en grado suficiente, de modo que quedaran comprendidos no solo los delitos basados en la cibernética, sino también otros delitos que con frecuencia se cometen utilizando internet y medios electrónicos (delitos facilitados por la cibernética), como el fraude cibernético, el robo cibernético, la extorsión, el blanqueo de dinero el tráfico de drogas y armas, la pornografía infantil y actividades terroristas.
>
> [...]
>
> s) Las organizaciones no gubernamentales y el mundo académico también deben implicarse en la labor de prevención y lucha contra la ciberdelincuencia, por cuanto aportan una perspectiva inclusiva, multifacética y amplia con la finalidad, entre otros, de garantizar la protección de derechos humanos, especialmente la libertad de expresión y el derecho a la vida privada.
>
> [...]
>
> ss) Algunos oradores recomendaron que la negociación y aprobación de una convención de las Naciones Unidas para promover la cooperación en la lucha contra el delito cibernético facilitara una cooperación internacional más eficiente en la lucha contra la ciberdelincuencia.

En cuanto al área de prevención, resalto la labor pedagógica y formativa a todo nivel -educativo elemental como de especialización-, así como los esfuerzos para identificar y compartir información relacionada al uso de las criptomonedas y ciberdelitos que van en aumento como el *phishing* y el *ransomware*:

219 El Grupo de Expertos sesionó en Viena, Austria, entre el 27 y el 29 de julio de 2020.

[...]

d) La sensibilización sobre la ciberseguridad debería incluirse como asignatura en la enseñanza primaria, secundaria y terciaria, tanto para los estudiantes como para los docentes. Lo ideal sería que esto formara parte de una estrategia nacional de ciberseguridad [...]

[...]

j) Los Estados deberían impartir capacitaciones para magistrados y jueces especializados que se ocupan de los casos de delito cibernético, y proporcionar a los órganos de investigación instrumentos de alto rendimiento para rastrear las criptomonedas y hacer frente a su utilización con fines delictivos.

[...]

o) Se alienta a los Estados miembros a que sigan incluyendo medidas de prevención eficaces en los planos nacional e internacional y a que se centren en actividades proactivas, como la sensibilización sobre los peligros del delito cibernético, realizando campañas relativas específicamente a los *modus operandi*, como el *phishing* o los programas maliciosos ("programas secuestradores"), y dirigidas a diferentes grupos, como los jóvenes o las personas de edad. También se alienta a los Estados miembros a que continúen centrándose en la probabilidad de enjuiciamiento y castigo de los delincuentes y los esfuerzos para prevenir el delito mediante la detección y el desbaratamiento de las actividades en curso de carácter ilícito en línea. Los servicios de policía y de fiscalía deberían invertir en detectar y señalizar las amenazas de la ciberdelincuencia y reaccionar a ellas. La colaboración entre el sector público y el privado es indispensable. Esas actividades de prevención no requieren leyes o reglamentos adicionales.

[...]

mm) Se recomendó la creación de una base de datos mundial sobre los abusos relacionados con las criptomonedas y la explotación de datos por los delincuentes en gran escala, así como la elaboración de un panorama general estratégico, coordinado a nivel mundial, de las amenazas que plantean las infracciones penales cometidas en la internet oscura.

2.6.9. XIV Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, 2021[220]

En el último congreso, celebrado en la ciudad de Kioto, se remarcó la preocupación existente entre los miembros de la Asamblea por el uso de las TIC para la comisión de delitos por parte de la criminalidad organizada, así como la aparición o consolidación de nuevas modalidades delictivas a partir del aislamiento obligatorio producto del COVID-19. Sin embargo, también se destacó la importancia del uso de las TIC por parte de los operadores jurídicos para combatir estos nuevos fenómenos delictivos. De la Declaración de Kioto sobre la Promoción de la Prevención del Delito, la Justicia Penal y el Estado de Derecho. Hacia el Cumplimiento de la Agenda 2030 para el Desarrollo Sostenible, destaco los siguientes pronunciamientos:

> 2. Expresamos también profunda preocupación por el hecho de que la delincuencia sea cada vez más transnacional, organizada y compleja, y de que los delincuentes aprovechen cada vez más las tecnologías nuevas y emergentes, entre ellas Internet, para llevar a cabo sus actividades ilícitas, lo que crea retos sin precedentes para prevenir y combatir los delitos existentes, así como formas nuevas y emergentes de delincuencia;
>
> [...]
>
> 8. Nos comprometemos a que nuestras instituciones encargadas de hacer cumplir la ley, de la justicia penal y otras instituciones pertinentes empleen de forma eficaz y apropiada las tecnologías nuevas y avanzadas como instrumentos para combatir la delincuencia con salvaguardias adecuadas y eficaces para prevenir el uso indebido y el abuso de dichas tecnologías en este sentido.
>
> [...]
>
> 13. Expresamos grave preocupación por la situación derivada de la enfermedad por coronavirus (COVID-19) y sus implicancias sociales y económicas, que han creado nuevas oportunidades para los delincuentes y los grupos delictivos organizados y han transformado sus *modus operandi* en diferentes grados, y también han planteado retos a la justicia en múltiples aspectos;

220 El XIV Congreso se llevó a cabo en Kioto, Japón, entre el 7 y el 12 de abril de 2021.

[...]

16. Reconocemos, a la luz de la experiencia en curso de la pandemia de COVID-19, y en preparación para otros desafíos similares que puedan presentarse en el futuro, la necesidad de revisar los sistemas de justicia penal y hacer que sean más eficaces, responsables, transparentes, inclusivos y receptivos mediante la promoción de la digitalización.

En las mesas redondas se discutieron diversos temas, entre ellos, la dificultad que representa para la investigación de los delitos cometidos en línea, el uso de las criptomonedas y las tecnologías de cifrado. Además, se destacó el desarrollo de una economía sumergida alrededor del robo de identidad y la venta de datos robados, las nuevas oportunidades de explotación en el ámbito de la trata de personas y el tráfico de migrantes a través del uso de internet, las redes sociales y los juegos *online*. En estas mesas de trabajo también se destacaron las ventajas de combinar la inteligencia artificial con la comunicación directa con las autoridades responsables de la cooperación internacional en materia penal, la toma de decisiones, el análisis forense, los modelos de actividad policial y los sistemas de vigilancia existentes.

2.6.10. La Convención de las Naciones Unidas contra la Ciberdelincuencia, 2024[221]

El 8 de agosto de 2024, en Nueva York, el comité especial encargado de elaborar una Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con fines delictivos[222] aprobó el "Proyecto de Convención de las Naciones Unidas contra la ciberdelincuencia: Fortalecimiento de la cooperación internacional para la lucha contra delitos cometidos mediante sistemas de tecnología de la información y las comunicaciones y para la transmisión de pruebas en forma electrónica de delitos graves".

221 El XIV Congreso se llevó a cabo en Kioto, Japón, entre el 7 y el 12 de abril de 2021.

222 Este comité fue establecido mediante Resolución N.º 74/247 del 27 de diciembre de 2019 por la Asamblea General de las Naciones Unidas. En la Resolución N.º 75/282 del 26 de mayo de 2021, se acordó que la primera sesión del Comité se llevaría a cabo en enero de 2022.

Se esperaba que este proyecto fuese aprobado a fines del 2024, con lo que se erigiría como el primer instrumento legalmente vinculante sobre la ciberdelincuencia[223].

Así, en la 55 sesión plenaria del 24 de diciembre de 2024, la Asamblea General de las Naciones Unidas adoptó la Convención de las Naciones Unidas contra la Ciberdelincuencia -el primer tratado de la Organización en el ciberespacio y el primero en justicia penal en más de 20 años-. La declaración de la directora ejecutiva de UNODC refleja la importancia histórica de esta convención:

> Acojo con satisfacción la histórica aprobación por la Asamblea General de las Naciones Unidas de una nueva convención internacional sobre ciberdelincuencia.
>
> Este notable paso representa el primer instrumento jurídico internacional de las Naciones Unidas en materia de delincuencia en los últimos 20 años, y llega en el momento oportuno.
>
> La tecnología es transformadora y está tendiendo puentes extraordinarios a través de fronteras y barreras, abriendo nuevos caminos para la humanidad.

223 Las palabras de la Directora Ejecutiva de UNODC, Sra. Ghada Waly, reflejan la importancia de este evento: "La finalización de esta Convención es un acontecimiento histórico, ya que se trata del primer tratado multilateral contra el crimen en más de 20 años y la primera Convención de las Naciones Unidas contra la Ciberdelincuencia, en un momento en que las amenazas en el ciberespacio crecen rápidamente [...] Felicito a los Estados Miembro y al Comité Ad Hoc, bajo el liderazgo de la Embajadora Faouzia Boumaiza-Mebarki como presidenta y destacada representante de las mujeres diplomáticas, por guiar las negociaciones y alcanzar un consenso sobre el texto final. En UNODC estamos inmensamente orgullosos de haber apoyado el proceso de negociación y de servir como secretaría de la convención. Continuaremos desempeñando un papel central apoyando la implementación y ratificación de la convención, una vez adoptada por la Asamblea General, además de proporcionar asistencia técnica a los Estados Miembro, a medida que trabajamos con todos los países y aliados para salvaguardar los espacios digitales" (Unodc. *Estados Miembro de las Naciones Unidas aprueban borrador para una convención contra la ciberdelincuencia*", 09 de agosto de 2024. https://www.unodc.org/lpomex/es/noticias/agosto-2024/estados-miembro-de-las-naciones-unidas-aprueban-borrador-para-una-convencion-contra-la-ciberdelincuencia.html).

> Pero los cibercriminales están haciendo un mal uso de esos avances, y la ciberdelincuencia es cada día más omnipresente y destructiva.
>
> En esta era de inteligencia artificial, encriptación *blockchain* y servicios digitalizados, la ciberdelincuencia está encontrando nuevos espacios que explotar.
>
> Está dando lugar a nuevas formas de delincuencia y amplificando sus formas tradicionales, perturbando las economías y las industrias.
>
> Se dirige a los más vulnerables y socava los Objetivos de Desarrollo Sostenible.
>
> Está erosionando la confianza en nuestra infraestructura digital, en nuestras instituciones y entre las personas, y se está desplazando a través de las jurisdicciones como nunca antes.
>
> La necesidad de cooperación y acción nunca ha sido mayor.
>
> Es por esto por lo que la nueva convención internacional sobre ciberdelincuencia es un paso histórico.
>
> La nueva convención es la base para una legislación y unos procedimientos penales más eficaces, así como para una mayor cooperación internacional.
>
> También proporcionará una hoja de ruta para las medidas preventivas y la asistencia técnica.
>
> La Oficina de las Naciones Unidas contra la Droga y el Delito está lista para trabajar con países y socios en la puesta en marcha de esta importante convención.
>
> Salvaguardando los espacios digitales, podemos construir un mundo más seguro para todos[224].

La Convención persigue como finalidad, prevenir y combatir la ciberdelincuencia a través del fortalecimiento de medidas legales, de la cooperación internacional y de la asistencia técnica. Los 68 artículos[225] que la integran se encuentran divididos en nueve capítulos:

224 Cfr. *Adopción de la convención de las Naciones Unidas contra la ciberdelincuencia.* https://www.unodc.org/ropan/es/Noticias/2024_diciembre_ciberdelito_convencion.html

225 Los siguientes artículos fueron acordados *ad referendum*: 5, 8, 10, 11, 15, 17, 18, 19, 20, 21, 22, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 36, 37, 38, 39, 44, 45, 46, 47, 48, 49, 50, 51, 52, 55, 56, 58, 59, 61, 63, 64, 67 y 68.

Capítulo	Artículo
Cap. I. Disposiciones generales	Art. 1. Finalidad
	Art. 2. Definiciones
	Art. 3. Ámbito de aplicación
	Art. 4. Delitos tipificados con arreglos a otros tratados y protocolos de las Naciones Unidas
	Art. 5. Protección de la soberanía
	Art. 6. Respeto de los derechos humanos
Cap. II. Criminalización	Art. 7. Acceso ilícito
	Art. 8. Interceptación ilícita
	Art. 9. Interferencia con datos electrónicos
	Art.10. Interferencia con un sistema de tecnología de la información y las comunicaciones
	Art. 11. Uso indebido de dispositivos
	Art. 12. Falsificación relacionada con un sistema de tecnología de la información y las comunicaciones
	Art. 13. Robo o fraude relacionado con un sistema de tecnología de la información y las comunicaciones
	Art. 14. Delitos relacionados con material en línea que muestra abusos sexuales de niños o explotación sexual de niños
	Art. 15. Instigación o captación con el fin de cometer un delito sexual contra un niño
	Art. 16. Difusión no consentida de imágenes de carácter íntimo
	Art. 17. Blanqueo del producto del delito
	Art. 18. Responsabilidad de las personas jurídicas
	Art. 19. Participación y tentativa
	Art. 20. Prescripción
	Art. 21. Enjuiciamiento, fallo y sanciones
Cap. III. Jurisdicción	Art. 22. Jurisdicción
Cap. IV. Medidas procesales y aplicación de la ley	Art. 23. Ámbito de aplicación de las medidas procesales
	Art. 24. Condiciones y salvaguardas
	Art. 25. Conservación acelerada de datos electrónicos almacenados
	Art. 26. Conservación acelerada y revelación parcial acelerada de datos relativos al tráfico
	Art. 27. Orden de presentación
	Art. 28. Búsqueda e incautación de datos electrónicos almacenados
	Art. 29. Obtención en tiempo real de datos relativos al tráfico
	Art. 30. Interceptación de datos relativos al contenido
	Art. 31. Embargo preventivo, incautación y decomiso del producto del delito
	Art. 32. Establecimiento de antecedentes penales
	Art. 33. Protección de testigos
	Art. 34. Asistencia y protección a las víctimas

Capítulo	Artículo
Cap. V. Cooperación internacional	Art. 35. Principios generales de la cooperación internacional
	Art. 36. Protección de datos personales
	Art. 37. Extradición
	Art. 38. Traslado de personas condenadas a cumplir una pena
	Art. 39. Remisión de actuaciones penales
	Art. 40. Principios generales y procedimientos relativos a la asistencia judicial recíproca
	Art. 41. Red 24/7
	Art. 42. Cooperación internacional a los efectos de la conservación acelerada de datos electrónicos almacenados
	Art. 43. Cooperación internacional para fines de revelación acelerada de datos relativos al tráfico conservados
	Art. 44. Asistencia judicial recíproca para el acceso a datos electrónicos almacenados
	Art. 45. Asistencia judicial recíproca para la obtención en tiempo real de datos relativos al tráfico
	Art. 46. Asistencia judicial recíproca para la interceptación de datos relativos al contenido
	Art. 47. Cooperación en materia de aplicación de la ley
	Art. 48. Investigaciones conjuntas
	Art. 49. Mecanismos de recuperación de bienes mediante la cooperación internacional para fines de decomiso
	Art. 50. Cooperación internacional para fines de decomiso
	Art. 51. Cooperación especial
	Art. 52. Devolución y disposición del producto del delito o de los bienes decomisados
Cap. VI. Medidas preventivas	Art. 53. Medidas preventivas
Cap. VII. Asistencia técnica e intercambio de información	Art. 54. Asistencia técnica y fomento de la capacidad
	Art. 55. Intercambio de información
	Art. 56. Aplicación de la Convención mediante el desarrollo económico y la asistencia técnica
Cap. VIII. Mecanismos de aplicación	Art. 57. Conferencia de los Estados parte en la Convención
	Art. 58. Secretaría
Cap. IX. Disposiciones finales	Art. 59. Aplicación de la Convención
	Art. 60. Efectos de la Convención
	Art. 61. Relación con los protocolos
	Art. 62. Aprobación de protocolos complementarios
	Art. 63. Solución de controversias
	Art. 64. Firma, ratificación, aceptación, aprobación y adhesión
	Art. 65. Entrada en vigor
	Art. 66. Enmienda
	Art. 67. Denuncia
	Art. 68. Depositario e idiomas

Capítulo	Artículo
Anexo. Notas interpretativas sobre artículos específicos de la Convención	Art. 2
	Art. 17
	Art. 23 y 35, en relación con el término "investigación"
	Art. 35

Cuadro 10: Cuadro resumen de la Convención de las Naciones Unidas contra la ciberdelincuencia. Elaboración propia.

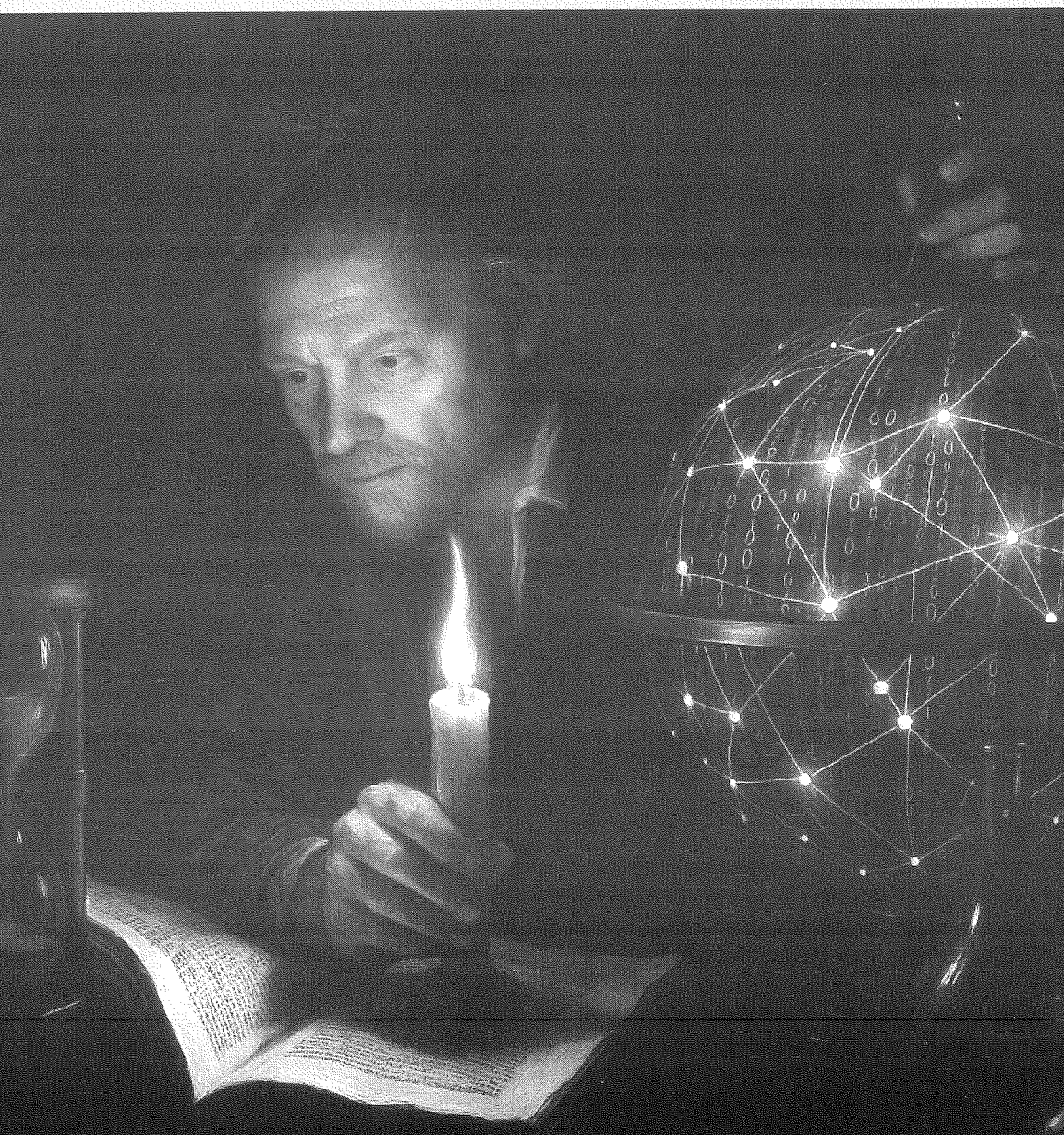
2.7. CONCLUSIONES DEL CAPÍTULO

- Desde los primeros ataques informáticos hasta las amenazas actuales, la evolución de la ciberdelincuencia ha demostrado que es un desafío que traspasa fronteras. En este sentido, la cooperación internacional es fundamental para prevenir, investigar y sancionar los delitos informáticos.
- Los primeros ataques informáticos revelaron la vulnerabilidad de los sistemas: en 1903, el mago Nevil Maskelyne realizó la primera demostración de un ataque informático al interceptar una transmisión de Marconi. Décadas después, René Carmille, considerado el primer *hacker*, utilizó la tecnología para alterar bases de datos y salvar vidas durante la Segunda Guerra Mundial. En 1971, el gusano *Creeper* marcó el nacimiento de los virus informáticos y, con ello, la necesidad de herramientas de ciberseguridad.
- La investigación académica sentó las bases para la regulación y sanción de la delincuencia informática. En los años setenta, Donn B. Parker catalogó más de 1000 casos de ciberdelincuencia, destacando la necesidad de normativas específicas. Poco tiempo después, Susan Hubell Nycum advirtió que la legislación tradicional no era suficiente para enfrentar la delincuencia informática.
- A nivel histórico, es importante reconocer los primeros marcos legislativos nacionales que iniciaron la lucha contra la ciberdelincuencia: Suecia (1973) fue el primer país en sancionar la alteración de datos informáticos en su Data Protection Act. Alemania (1980) y Canadá (1985) incluyeron el fraude informático en sus códigos penales. Estados Unidos (1986) aprobó la primera ley federal contra la ciberdelincuencia, sentando un precedente en la regulación.

- Europa lideró los esfuerzos iniciales de armonización legislativa. En 1981, el Convenio N.º 108 del Consejo de Europa estableció medidas de protección de datos personales. En 1989, la Recomendación N.º R (89) 9 sugirió una lista mínima de ciberdelitos que deberían tipificarse en las legislaciones nacionales. En el 2001, el Convenio de Budapest fue el primer tratado internacional vinculante sobre ciberdelincuencia, abordando delitos como acceso ilícito, fraude informático y pornografía infantil.
- América también adoptó un enfoque regional para combatir la cibercriminalidad. Así, a partir de 1997, la OEA incluyó la ciberdelincuencia en su agenda de seguridad. La REMJA promovió la armonización legislativa y la cooperación en investigaciones transfronterizas. De este modo, se recomendó la creación de unidades especializadas en cibercriminalidad en los países miembros.
- La evolución de la regulación internacional ha respondido a nuevos desafíos. En el 2003, se adoptó un protocolo adicional al Convenio de Budapest para penalizar delitos de odio en línea. En el 2007, el Convenio de Lanzarote incluyó el *grooming* como delito informático para anticiparse y mejorar la protección de la libertad e indemnidad sexual de los menores de edad. En el 2016, la directiva europea 2016/680 reforzó la seguridad de los datos personales y estableció sanciones para su uso indebido. Finalmente, en el 2022, se firmó el Segundo Protocolo Adicional al Convenio de Budapest, ampliando la cooperación internacional y facilitando el acceso a pruebas digitales.
- Poco a poco, Latinoamérica avanza en la adhesión a instrumentos internacionales de lucha contra la ciberdelincuencia. Así, a inicios del 2025, diez países de la región han ratificado el Convenio de Budapest, incluyendo Argentina, Brasil, Chile, Colombia y Perú. Es importante resaltar que los marcos normativos locales se han adaptado progresivamente para sancionar los delitos informáticos y, además, mejorar los mecanismos de cooperación internacional.

CAPÍTULO 3

HISTORIA LEGISLATIVA DE LOS DELITOS CONTRA LA SEGURIDAD INFORMÁTICA



* La ilustración de la página anterior corresponde a una adaptación de *El astrónomo a la luz de la vela, de Gerrit Dou. Para su elaboración, se empleó una de las herramientas de generación de imágenes de la empresa OpenAI.*

CAPÍTULO 3

HISTORIA LEGISLATIVA DE LOS DELITOS CONTRA LA SEGURIDAD INFORMÁTICA*

Sumario: 3.1. Introducción. 3.2. Primer periodo: de 1991 al 2000. 3.3. Segundo periodo: de 2000 al 2013. 3.4. Tercer periodo: de 2013 a diciembre de 2023. 3.5. Cuarto periodo: de diciembre del 2023 a la actualidad. 3.6. Conclusiones del capítulo.

3.1. INTRODUCCIÓN

[Caso 49] Mayo del 2000, Renato llega a casa, prende su computadora y se conecta a internet. Revisa su correo y un mensaje en particular le llama la atención: «I LOVE YOU». Abre el *mail* y descarga el archivo «Love-Letter-For-You.TXT.VBS» -cuya traducción al español es 'carta de amor para ti'-. Renato se sorprende al descubrir que diversos archivos de su computadora se habían dañado y que desde su correo se enviaron mensajes similares a toda la lista de sus contactos. ¿Qué ocurrió?

Renato fue víctima de un gusano de red que, según los informes de Kaspersky, solo el primer día de su lanzamiento, 4 de mayo de 2000, infectó miles de sistemas. Cinco días después, alcanzó los 2.5 millones, logrando

* Algunos comentarios y reflexiones fueron inicialmente publicadas en ELÍAS PUELLES, Ricardo. "Luces y sombras en la lucha contra la delincuencia informática en el Perú". En: DUPUY, Daniela (dir.) y Mariana KIEFER (coord.). *Cibercrimen. Aspectos de derecho penal y procesal penal. Cooperación internacional. Recolección de evidencia digital. Responsabilidad de los proveedores de servicios de Internet*. Montevideo: B de F, 2019.

comprometer, en poco tiempo, el 10 % de sistemas, a nivel mundial. Se estima que este gusano ocasionó 10 mil millones de dólares en pérdidas, pues no solo generaba *spam*, sino que, además, descargaba un troyano que enviaba las contraseñas de correo del usuario y eliminaba o corrompía archivos almacenados en el disco duro[226].

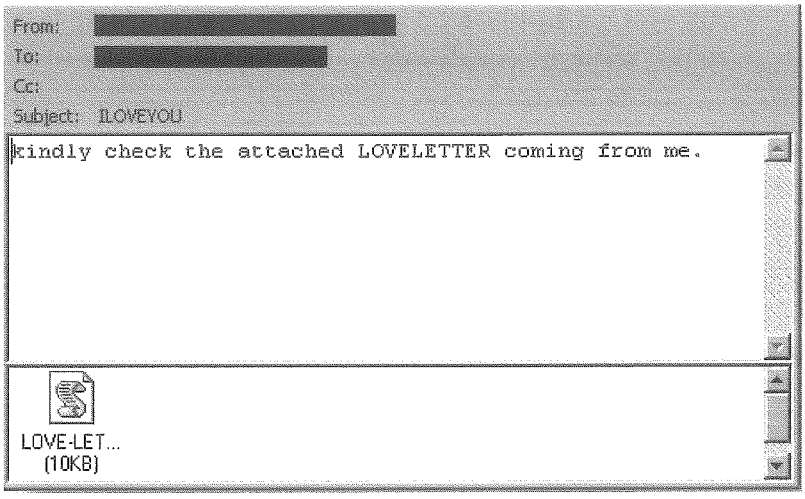


Imagen 7. Correo electrónico dirigido a la víctima, cuyo asunto es «ILOVEYOU» y al que se adjunta el gusano informático[227].

A fines de los noventa, conscientes del impacto de la tecnología, juristas destacados, como el profesor Luis Bramont-Arias, avizoraban con plena lucidez el futuro del derecho penal:

> El desarrollo tecnológico ha sido tan importante en los últimos tiempos que la interpretación tradicional de las clásicas figuras delictivas del Derecho Penal ha quedado completamente obsoleta ante este nuevo fenómeno representado por la criminalidad informática.

226 Root, Enoch, "ILOVEYOU: el virus que amaba a todo el mundo", en *Kaspersky Daily*, 11 de agosto de 2022. https://www.kaspersky.es/blog/cybersecurity-history-iloveyou/27485/

227 La imagen fue tomada de Root, "ILOVEYOU: el virus que amaba a todo el mundo", cit.

> Ante esta situación, el legislador se sitúa ante una doble opción, o crear nuevos tipos penales donde se criminalicen específicamente estas conductas, como delitos autónomos, o bien, introducirlas como modalidades de comisión dentro de las conductas delictivas ya tipificadas. Esta última posición es la asumida específicamente por el Código Penal peruano[228].

En este capítulo, analizaré la historia y evolución de la legislación peruana especializada en el cibercrimen, específicamente aquella relacionada con los ataques contra la seguridad informática. De este modo, omitiré cualquier referencia a otro tipo de delincuencia informática, como aquella que atenta contra el patrimonio -estafa en entornos virtuales y fraude informático-, contra la libertad e indemnidad sexual -*grooming* y distribución de material de abuso sexual infantil-, contra la fe pública -suplantación de identidad-, contra la libertad personal -acoso virtual-, entre otros[229].

Por esta razón, con estrictos fines metodológicos, he dividido esta evolución histórica en cuatro periodos:

- El primer periodo inicia con la promulgación del Código Penal (1991) y concluye con la inclusión y tipificación de los delitos informáticos (2000).
- El segundo periodo empieza en el 2001 y termina con la promulgación de la Ley de Delitos Informáticos (2013). Dado el volumen de información y su relevancia, dividí esta etapa en dos secciones: (i) proyectos de ley que no fueron aprobados y (ii) leyes que modificaron el Código Penal durante la década analizada.
- El tercer periodo inicia el 22 de octubre de 2013, fecha en la que se publicó la Ley de Delitos Informáticos y finaliza en diciembre de 2023.

228 Bramont-Arias Torres, Luis Alberto. *El delito informático en el Código Penal peruano*. Lima: Fondo Editorial de la Pontificia Universidad Católica del Perú, 1997, p. 79.

229 La historia general de la ciberdelincuencia peruana puede ser consultada en: Elías Puelles, Ricardo. "La evolución del cibercrimen en el Perú. De hurto telemático a ataques contra sistemas informáticos". En: Espinoza Calderón, Víctor Raúl (coord.). *Cibercriminalidad y delitos informáticos*. Lima: Instituto Pacífico, 2023, pp. 39-85.

- El cuarto periodo empieza el 13 de diciembre del 2023, fecha en la que se publicó el Decreto Legislativo N.° 1591, norma que modificó la Ley de Delitos Informáticos, y comprende hasta la actualidad.

Espero que este capítulo sea útil, no solo para el especialista que desea conocer el desarrollo normativo de los últimos 34 años, sino también para el ciudadano que quiere identificar y reconocer a los hombres y mujeres que se encuentran detrás de tan importantes cambios legislativos.

3.2. PRIMER PERIODO: DE 1991 AL 2000

El Código Penal peruano fue promulgado el 3 de abril de 1991 y ya avizoraba la importancia de sancionar los delitos cometidos a través de las TIC. Por esta razón, desde que entró en vigor, tipificó y sancionó el delito de hurto telemático[230], bajo tres modalidades: (i) uso de sistemas de transferencia electrónica de fondos, (ii) uso de la telemática o (iii) violación de claves de secretas. Además, como veremos a continuación, identificó un tipo de delito que atenta contra el derecho a la intimidad y, en especial, contra el secreto de las comunicaciones: la interferencia telefónica.

230 "Es preciso denotar que, el delito de hurto calificado por transferencia electrónica de fondos tiene directa implicancia en la actividad informática. En la doctrina y legislación comparada, esta figura delictiva está generalmente tipificada como fraude informático; en la legislación peruana, la aplicación de la figura del hurto al caso de las manipulaciones informáticas debe ser materia de revisión y de mayores estudios e investigación" (Blossiers Hüme, Juan José. *Criminalidad informática*. Lima: Editorial Portocarrero, 2003, p. 162). Sobre las formas de ejecución de la conducta típica: Bramont-Arias Torres, *El delito informático en el Código Penal peruano*, cit., pp. 68-70. Cierto sector de la doctrina recuerda que este delito no emerge como un delito autónomo sino como una agravante: Jiménez Herrera, Juan Carlos. *Manual de derecho penal informático*. Lima: Jurista, 2017, p. 396; Villavicencio Terreros, Felipe. "Delitos informáticos". En: *Ius et Veritas* 49. Lima: 2014, p. 287. Sobre los antecedentes de los delitos informáticos en Perú: Villavicencio Terreros, Felipe. "Los delitos informáticos en la legislación penal peruana". En: Riquert, Marcelo A. (dir.) y Carlos Christian Sueiro (coord.). *Sistema penal e informática. Ciberdelitos. Evidencia digital. TICS*, vol. 1. Buenos Aires: Hammurabi, 2019, pp. 274 y s.

3.2.1. La interferencia telefónica (art. 162 CP), 1991

En lo que a la seguridad informática se refiere, desde su promulgación y ubicándolo en el capítulo IV, denominado "Violación del secreto de las comunicaciones", el Código Penal tipificó y castigó el delito de interferencia telefónica, estableciendo dos modalidades: (i) la interferencia y (ii) la escucha de las conversaciones telefónicas o similares:

> **Art. 162 CP.**- El que, indebidamente, interfiere o escucha una conversación telefónica o similar será reprimido con pena privativa de libertad no menor de uno ni mayor de tres años.
>
> Si el agente es funcionario público, la pena privativa de libertad será no menor de tres ni mayor de cinco años e inhabilitación conforme al art. 36, incisos 1, 2 y 4.

El arribo de la telefonía móvil (1990)[231] y la rápida masificación del uso del internet (1992)[232] en Perú trajo nuevas modalidades delictivas. Así, en menos de una década, el problema del empleo indebido de las TIC ocasionó que el Congreso decidiera sancionar a quienes las empleaban con fines ilícitos. La primera respuesta de nuestro legislador fue la tipificación de los delitos informáticos. Posteriormente, al no ser suficiente, se crearon nuevos delitos o se agravaron los ya existentes con la finalidad de perseguir a aquellos delincuentes que empleaban este tipo de tecnologías como un medio para la perpetración de otros como el turismo sexual, la distribución de imágenes o videos de abuso sexual infantil -mal llamada *pornografía infantil*-, fraude electrónico, apología al terrorismo a través de entornos digitales, etcétera.

231 "La historia de la revolución de la telefonía móvil en el Perú", en *El Comercio*, Lima, 6 de febrero de 2015. https://elcomercio.pe/economia/negocios/historia-revolucion-telefonia-movil-peru-330906-noticia/

232 "Día de internet: Le evolución de la red en el Perú", en *El Comercio*, Lima, 17 de mayo de 2017. https://elcomercio.pe/economia/dia-internet-evolucion-red-peru-423057-noticia/

La norma bajo comentario permaneció inmutable hasta el 22 octubre del 2013, fecha en la que fue modificada por la Cuarta Disposición Complementaria Modificatoria de la LDI. Luego de ello, recibiría dos actualizaciones más[233].

3.2.2. Tipificación de los delitos informáticos (arts. 207-A, 207-B y 207-C CP), 2000

Nuestro país comenzó a participar en el uso de la internet en diciembre de 1991, siendo la Red Científica Peruana (RCP) precursora de este fenómeno. Sin embargo, no fue sino hasta 1994, gracias a la RCP, Infovía y la aparición de los primeros centros proveedores de internet, que su uso se comenzó a masificar[234]. Si bien en los años siguientes no se informó sobre el auge o proliferación de los cibercrímenes, el sector empresarial sí se mostró preocupado, pues, de un lado, el nivel de protección de los correos electrónicos, bases de datos y pioneras páginas web era ínfimo[235] y, de otro, no contábamos con legislación que castigara estas nuevas conductas ilícitas.

Los primeros debates registrados en el Perú en torno a los delitos informáticos se originaron en el último semestre de 1999, tras la presentación de los Proyectos de Ley N.º 5071, 5132 y 5326 por los congresistas Jorge Muñíz Ziches, Susana Díaz Díaz[236] y Anastacio Vega Ascencio, respectivamente. Los dos primeros proyectos

233 Estas modificaciones se efectuaron por medio de la Ley N.º 30171 del 10 de marzo de 2014 y del Decreto Legislativo N.º 1182 del 27 de julio de 2015.

234 De acuerdo al Organismo Supervisor de la Inversión Privada en Telecomunicaciones (Osiptel), se pasó de 500 a 600 mil accesos a Internet entre 1994 y 1997. Sin embargo, según INEI, solo el 3 % de los hogares a nivel nacional tenían conexión a internet (cfr. *Business. Negocios en el Perú*. Año 5. N.º 42, marzo, Lima: 1998, p. 18).

235 La revista *Business* realizó una encuesta en abril de 1998 entre 250 ejecutivos peruanos y detectó que al 79,2 % de los encuestados les preocupa la privacidad de sus comunicaciones por email. El 52,6 % utilizaban solo un método de seguridad; mientras que un 36,8 %, dos mecanismos; y un 10,6 %, de tres a cinco métodos –entre ellos, contar con un *password* para la PC y otra para la cuenta de correo electrónico, utilizar su cuenta en una computadora de uso personal, así como guardar sus mensajes en disquetes (cfr. *Business. Negocios en el Perú*. Año 5. N.º 43, abril, Lima: 1998, pp. 62 y s.).

236 La congresista Susana Díaz Díaz, previamente, presentó el proyecto de Ley N.º 4957 del 6 de julio de 1999, titulado "Ley de Delitos Informáticos", el cual fue enviado al archivo el 6 de agosto del mismo año.

guardan relación con la seguridad informática; mientras que el tercero, con el patrimonio -razón por la que no está incluido en este estudio-:

2.1 El proyecto de Ley N.º 5071/99 del 18 de agosto de 1999 recomendó incorporar los delitos de acceso ilícito (art. 208-A CP[237]) y de sabotaje informático (art. 209-B CP[238]) al Código Penal. Resulta curiosa la aclaración recogida en su exposición de motivos, pues demuestra la incipiente aproximación inicial de esta temprana época: "Que, los llamados delitos informáticos no son cometidos por la computadora, sino que es el hombre quien los comete con la ayuda de aquella. En este sentido, el presente proyecto se dirige a la regulación penal de las posibles medidas preventivas de carácter penal que consideramos deben ser tomadas en cuenta para evitar que la comisión de este tipo de delitos, alcance en el país los niveles de peligrosidad que se han dado en otros países".

2.2 El proyecto de Ley N.º 5132/99 del 31 de agosto de 1999 propuso la creación de la LDI, la cual recogería cuatro ilícitos: atentado contra sistemas informáticos (art. 1[239]), acceso ilícito (art. 2[240]), atentado contra datos informáticos (art. 3[241]) y difusión de datos informáticos

237 Proyecto de Ley N.º 5071/99, art. 208-A.- El que indebidamente utilice o ingrese a una base de datos, sistema o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio con el fin de defraudar, obtener dinero, bienes o información será reprimido con pena privativa de libertad no mayor de dos años, o con prestación de servicios comunitarios de cincuenta y dos a ciento cuatro jornadas.

238 Proyecto de Ley N.º 5071/99, art. 209-B.- El que indebidamente interfiera, reciba, utilice, altere, dañe o destruya un soporte o programa de computadora o los datos contenidos en la misma, en la base, sistema o red será reprimido con pena privativa de libertad no mayor de dos años.

239 Proyecto de Ley N.º 5132/99, art. 1.- El que maliciosamente destruya o inutilice el soporte lógico de un sistema computacional, empleando medios computacionales, será reprimido con pena privativa de libertad no mayor de cuatro años.

240 Proyecto de Ley N.º 5132/99, art. 2.- El que, con ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, lo interfiera o acceda a él, será reprimido con pena privativa de libertad no mayor de tres años.

241 Proyecto de Ley N.º 5132/99, art. 3.- El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será sancionado con pena privativa de libertad no mayor de cuatro años.

> (art. 4[242]). En la exposición de motivos, me parece interesante que la congresista Susana Díaz Díaz remarcara que nos encontramos, de un lado, frente a nuevo tipo de crímenes y, de otro, que los datos informáticos requieren especial protección: "[...] han surgido nuevas conductas, impensadas por el legislador de hasta hace medio siglo, que por su especial naturaleza no admiten encuadrarse dentro de las figuras convencionales informatizadas, sino que es necesario que se creen nuevos tipos. Son estos delitos a los que se les denomina delitos informáticos [...] El delito informático no atenta contra el hardware sino contra el soporte lógico, porque la especial naturaleza de los datos digitalizados y de los programas computacionales, su carácter intangible, no le permite al tipo penal tradicional cubrirlo haciendo necesario la creación de un nuevo delito".

Estas tres propuestas legislativas respondieron a la revolución informática-económica de su época[243], al contexto electoral en que se encontraban envueltos[244] y a la preocupación que trajo la interceptación de correos electrónicos suscitados en nuestro país[245].

Estas propuestas se cristalizaron en la Ley N.º 27309, promulgada el 17 de julio de 2000, que creó el delito informático[246] (art. 207-A CP), el delito

---

242 Proyecto de Ley N.º 5132/99, art. 4.- El que maliciosamente revele o difunda los datos de contenidos en un sistema de información sufrirá pena privativa de libertad no mayor de cuatro años. Si quien incurre en estas conductas es el responsable del sistema de información, la pena será no mayor a seis años.

243 Hacia julio de 1998, se señalaba que el fenómeno de delitos informáticos no se ha presentado con fuerza en el Perú, pues solo se detectaron algunos casos de *hackers* locales, cuyas operaciones se limitaron al uso de claves para entrar a sistemas que requerían pagar por obtener una suscripción (*Business. Negocios en el Perú*. Año 5. N.º 46, julio, Lima: 1998, p. 36).

244 En la sesión vespertina del 3 de mayo de 2000, al discutirse la creación de los delitos informáticos, se trajo a colación las elecciones presidenciales a realizarse en julio de ese año, pues se señaló que las penas resultaban demasiado benignas en caso de producirse la alteración en el sistema de cómputo que operaría en la segunda vuelta electoral.

245 En la misma sesión, para justificar que la sanción de los delitos informáticos debía equipararse a las de interceptación telefónica (tres años), se citó la interceptación de los correos electrónicos del congresista García-Sayán y su publicación en el *Diario Expreso*.

246 El delito informático ha recibido diferentes denominaciones en la doctrina penal peruana, tales como *hacking* lesivo, intrusismo informático y acceso informático indebido.

de alteración, daño y destrucción de base de datos, sistema, red o programa de computadoras[247] (art. 207-B CP) y el delito informático agravado (art. 207-C CP)[248]:

> **Art. 207-A CP.-** El que utiliza o ingresa indebidamente a una base de datos, sistema o red de computadoras o cualquier parte de la misma, para diseñar, ejecutar o alterar un esquema u otro similar, o para interferir, interceptar, acceder o copiar información en tránsito o contenida en una base de datos, será reprimido con pena privativa de libertad no mayor de dos años o con prestación de servicios comunitarios de cincuenta y dos a ciento cuatro jornadas.
>
> Si el agente actuó con el fin de obtener un beneficio económico, será reprimido con pena privativa de libertad no mayor de tres años o con prestación de servicios comunitarios no menor de ciento cuatro jornadas.
>
> **Art. 207-B CP.-** El que utiliza, ingresa o interfiere indebidamente una base de datos, sistema, red o programa de computadoras o cualquier parte de la misma con el fin de alterarlos, dañarlos o destruirlos, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años y con setenta a noventa días multa.
>
> **Art. 207-C CP.-** En los casos de los arts. 207-A y 207-B, la pena será privativa de libertad no menor de cinco ni mayor de siete años cuando:
>
> 1. El agente accede a una base de datos, sistema o red de computadora, haciendo uso de información privilegiada, obtenida en función a su cargo.
> 2. El agente pone en peligro la seguridad nacional.

247 Identificado en nuestro medio como *delito de sabotaje informático* o *de daño informático.*

248 Este art. no se encontraba regulado en los proyectos inicialmente discutidos por el Congreso, sino que fue producto de la séptima observación formulada por el Poder Ejecutivo, la cual fue aceptada y respaldada por el congresista Muñiz Ziches, Presidente de la Comisión de Reforma de Códigos. Ver. p. 920 del Diario de Debates del Congreso de la República del 21 de junio de 2000. Sobre los antecedentes de la Ley de Delitos Informáticos: Espinoza Calderón, Víctor Raúl. *Delitos informáticos y nuevas modalidades delictivas.* Lima: Instituto Pacífico, 2022, pp. 62 y s ; Arévalo Minchola, Maguín y J. A. Vega Aguilar, *Ciberdelitos. Análisis en el sistema penal.* Lima: Iustitia, 2022, pp. 213-230.

El art. 207-D CP denominado *tráfico ilegal de datos* se incorporó en agosto del 2013, pero, al igual que los art. 207-A, 207-B y 207-C fue derogado cuando en octubre de ese año, la LDI entró en vigor. Ahora bien, contextualizar esta implementación nos permite precisar algunos problemas generados, tanto con su incorporación al ordenamiento como con las propuestas de modificación posteriores:

a. El legislador asoció la criminalidad informática a la criminalidad patrimonial, razón por la cual su tipificación se incluyó en el Título V del Código Penal, correspondiente a los *Delitos contra el Patrimonio*. Esto se debió a que inicialmente se pensaba que estos ilícitos eran solo una extensión de lo que el Código Penal de 1991 preveía como agravantes en la comisión del hurto (utilización de sistemas de transferencia electrónicas de fondos, de la telemática en general o la violación del empleo de claves secretas). Por esta razón, algunos autores consideraron que estos delitos no formaban parte del Derecho Penal Económico ni que protegían la seguridad informática o la intimidad, pues identifican al patrimonio como el principal –o, en algunos casos, como el único– bien jurídico tutelado por estas normas. El agrupar en un solo capítulo conductas que en realidad protegían diversos bienes jurídicos generó un grave error: pensar que cualquier acto de intrusismo lesionaba el patrimonio de los agraviados[249]. De allí que, pese a las observaciones que el Poder Ejecutivo realizó, el Congreso reiteró que la finalidad de estos nuevos delitos era la protección del patrimonio de sus titulares[250].

b. Los delitos informáticos fueron catalogados como delitos de peligro y no de resultado. Así, en el debate previo a su aprobación, se señaló lo siguiente:

> El delito de peligro surge ya desde el ingreso a la utilización indebida de los elementos informáticos o a la información de las personas contenidas en los mismos o en las bases de datos, sea para sabotear, espiar, defraudar o dañar. Es decir, no se requiere

249 Salinas Siccha, Ramiro. *Derecho penal. Parte especial.* 3.ª edición. Lima: Grijley, 2008, pp. 1202 y 1210.

250 Congreso de la República. *Diario de los debates.* Sesión del 21 de junio de 2000, p. 921.

que se produzca un resultado para estar frente a un delito informático, pues basta la intención.[251]

c. El legislador acudió a las sanciones del Derecho Penal como *prima ratio*, pues evitó acudir a un ente administrativo que pueda sancionar conductas que por su escasa gravedad (cuantitativa o cualitativa) no merezcan el máximo reproche punitivo con el que cuenta el Estado. Además, promulgó las normas penales sin contar con personal técnico especializado que colaborase con las investigaciones preliminares o judiciales, lo que originó que muchos procesos queden impunes[252]. Así, la División de Investigación de Delitos de Alta Tecnología de la Policía Nacional del Perú se creó recién cinco años después de la promulgación de la Ley N.º 27309 y la Fiscalía Especializada en Cibercriminalidad del Ministerio Público, casi veinte años después.

3.3. SEGUNDO PERIODO: DEL 2000 AL 2013

3.3.1. Propuestas legislativas que no prosperaron

Luego de la incorporación de los delitos informáticos al CP, en cada periodo legislativo se presentaron diversas propuestas que buscaron endurecer las penas, crear nuevas modalidades delictivas, mejorar la redacción de los tipos penales siguiendo los lineamientos internacionales que, año a año, se venían desarrollando -y que han sido sistematizados en el capítulo anterior- o mejorar las unidades especiales a cargo de su investigación y juzgamiento.

3.3.1.1. Periodo legislativo 2000-2001

En este periodo se presentó solo un proyecto de ley sobre la materia bajo análisis. Así, se propuso adicionar la inhabilitación a las sanciones previstas en los recientemente incorporados delitos informáticos.

---

251 Congreso de la República, *Diario de los debates*, cit., p. 921.

252 En el mismo sentido, Mazuelos Coello, Julio F. "Los delitos informáticos: Una aproximación a la regulación del Código Penal peruano". En: *Revista Peruana de Doctrina y Jurisprudencia Penales* 2. Lima: Grijley, 2001, p. 292.

- El proyecto de Ley N.º 1744 del 3 de mayo de 2001, presentado por el congresista Rafael Castañeda Castañeda, sugirió agregar la inhabilitación prevista en el numeral 4 del artículo 36 CP a los artículos 207-A, 207-B y 207-C. La exposición de motivos no desarrolló los fundamentos, limitándose a señalar que "[c]on la ayuda de las nuevas tecnologías, aparecen nuevos delitos y nuevas formas de comisión de delitos. Frente a ello, es necesario legislar con prontitud y sancionar los actos ilícitos. Por ello, el tema de la criminalidad informática, que presenta una complejidad elevada, exige la creación de una regulación adecuada".

3.3.1.2. Periodo legislativo 2001-2006

En el periodo 2001-2006, se presentaron dos proyectos legislativos, los cuales estuvieron orientados a incrementar las penas de los delitos informáticos:

a. Proyecto de Ley N.º 2 226/2002, presentado el 13 de marzo de 2002 por los congresistas José Barba Caballero e Hildebrando Tapia Samaniego. Los legisladores propusieron aumentar la sanción prevista en los arts. 207-A CP y 207-B hasta seis años de pena privativa de libertad, mientras que en la figura agravada, artículo 207-C CP, hasta nueve años de pena privativa de libertad.

   La exposición de motivos del proyecto de ley no explica la relación del aumento de las sanciones con una lucha efectiva contra la ciberdelincuencia. Así, si bien se enumeran algunas características de este fenómeno delictivo -como las dificultades investigativas para descubrir al autor o las *cifras negras* que surgen al no denunciar estos hechos-, únicamente se señala que "la presente norma permitirá sancionar los actos ilícitos por delitos informáticos con penas más severas que mermen este acto delictivo".

b. Proyecto de Ley N.º 11402/2004, presentado el 10 de setiembre de 2004 por el legislador Juan de Dios Ramírez Canchari. En este caso, la propuesta únicamente tuvo como objetivo modificar el artículo 207-A CP, elevando la sanción prevista en el primer párrafo hasta cuatro años y, en el segundo, hasta seis años de pena privativa de libertad.

Este proyecto de ley equipara los efectos del delito informático previsto en el artículo 207-A CP con la estafa, regulada en el 196 CP, por cuanto en ambos casos el agraviado vería mermado su patrimonio. Bajo esta premisa, en la exposición de motivos, se justifica el incremento punitivo: "[...] su efecto disuasivo resultó insuficiente pues la incidencia delictiva utilizando este medio ha aumentado, sobre todo mediante los sistemas informáticos de las entidades bancarias que son vulnerados para apropiarse o disponer de los fondos que dichas instituciones custodian, sin que exista respuesta firme del Estado [...] Los autores de estos delitos no pueden ser condenados a prisión efectiva, cumplirán su sentencia gozando de libertad, situación que les ha permitido organizar o preparar la comisión de nuevos delitos, mientras que los afectados en la mayoría de los casos no recuperan sus depósitos [...] Por consiguiente, resulta necesario adecuar las penas previstas a la realidad actual considerando la magnitud del daño y el impacto social que producen, sin perder de vista que sus efectos son similares a los generados por el delito de estafa cuya sanción según la norma penal sustantiva alcanza los 06 años de pena privativa de libertad".

Además, este periodo legislativo registra dos proyectos de creación de nuevas modalidades de ciberdelincuencia relacionadas con la seguridad informática:

c. Proyecto de Ley N.º 7197, presentado el 13 de junio de 2003 por la congresista Martha Hildebrandt Pérez-Treviño. La autora de la propuesta advirtió un vacío normativo que permitiese castigar penalmente aquellos casos en los que se introducen redireccionamientos no deseados por el titular de una página web, por lo que sugiere la incorporación del artículo 207-D CP[253].

253 Proyecto de Ley N.º 7197, art. 207-D .- El agente que se sirve de páginas web de carácter privado, sin conocimiento de su titular, para crear vínculos con otras páginas web será reprimido con pena privativa de libertad no mayor de dos años o con prestación de servicios comunitarios de cincuenta y dos a ciento cuatro jornadas.
Si el agente actuó con el propósito de obtener un beneficio económico o con el de perpetrar otro delito, será reprimido con pena privativa de libertad no mayor de tres años o con prestación de servicios comunitarios no menor de ciento cuatro jornadas.

En la exposición de motivos, la congresista desarrolla dos supuestos de aplicación normativa[254].

d. Proyecto de Ley N.º 10079/2003, presentado el 17 de marzo de 2004 por el congresista Pedro Morales Mansilla y por el cual se pretendió modificar el artículo 207-B CP[255], así como incorporar al CP los artículos 207-D[256], 207-E[257],

254 "1) Personas que tienen relación con el propietario de una página web. Por ejemplo: una determinada persona solicita o contrata los servicios de un diseñador de páginas web. El diseñador, al confeccionar esa página, crea, sin conocimiento del contratante, un vínculo aparentemente imperceptible que lleva a otras páginas web de diverso género.
2) Personas que no tienen relación con el propietario de la página web. Por ejemplo: aquel individuo que, aprovechando sus conocimientos avanzados de informática, escoge una página web sin haber. participado en su confección para crear e introducir un vínculo, con otra (u otras) página web" (Proyecto de Ley N.º 7197, presentado el 13 de junio de 2003 por la congresista Martha Hildebrandt Pérez-Treviño).

255 Proyecto de Ley N.º 10079/2003, art. 207-B.- Son responsables de fraude informático las personas que, valiéndose de cualquier método o modo, alteren, interfieran, manipulen, modifiquen o utilicen el funcionamiento de un programa informático, sistema informático, red, telemático o un mensaje de datos para procurarse la transferencia no consentida de los bienes, valores, derechos o patrimonio de otra persona en perjuicio de ésta o de un tercero, serán sancionados con pena de privativa de libertad no menor de tres años ni mayor de cinco años y con noventa a ciento veinte días multa.

256 Proyecto de Ley N.º 10079/2003, art. 207-D.- Son responsables del delito de daños informáticos, la persona o personas que de cualquier modo o utilizando cualquier método destruyan, alteren, inutilicen, supriman o dañen los programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un soporte lógico, sistema de información o telemático, y serán reprimidas con pena privativa de libertad no menor de tres mayor de cinco años y con sesenta a ciento ochenta días multa.
Serán reprimidos con la pena privativa de la libertad no menor de cinco ni mayor de siete años y con sesenta a doscientos días multa, los que además destruyan o inutilicen la infraestructura e instalaciones físicas necesarias para la transmisión, recepción o codificación de los mensajes de datos.

257 Proyecto de Ley N.º 10079/2003, art. 207-E.- Son responsables de falsificación informática la persona o personas que, con ánimo de lucro, o bien para causar un perjuicio a un tercero, utilizando cualquier medio alteren o modifiquen mensajes de datos o la información incluida en estos, que se encuentre contenida en cualquier soporte material, sistema de información o telemático, ya sea:
1. Alterando un mensaje de datos en alguno de sus elementos o requisitos de carácter formal o esencial.
2. Simulando un mensaje de datos, en todo o en parte, de manera que induzca a error sobre su autenticidad.

207-F[258] y 207-G[259]. Rescato algunas ideas centrales recogidas en la exposición de motivos de esta propuesta normativa. En primer lugar, de forma adecuada resalta el valor de la información,

3. Suponiendo en un acto la intervención de personas que no la han tenido o atribuyendo a las que han intervenido en el acto, declaraciones o manifestaciones diferentes de las que hubieren hecho.
4. Faltando a la verdad en la narración de los hechos.

Cualquier alteración, falsificación, simulación, falsa suposición o imputación de un mensaje de datos, será reprimida con pena privativa de libertad no menor de tres ni mayor de cinco años y con sesenta a ciento ochenta días.

Si el delito es cometido por un funcionario público o de la entidad de certificación de información, la pena a imponerse podrá ser elevada hasta en un tercio por encima del máximo legal y además traerá consigo la pena accesoria de inhabilitación.

258 Proyecto de Ley N.º 10079/2003, art. 207-F.- Son responsables de intrusión indebida a los sistemas informáticos, de información o telemáticos la persona o personas que por cualquier medio o fin, y con el ánimo de apoderarse de la información contenida en dichos sistemas, o para descubrir los secretos comerciales o industriales, o bien para vulnerar la intimidad de una persona natural o jurídica, o simplemente vulnerar su seguridad, sin su consentimiento o autorización, interfieran, interrumpan, accedan a sistemas de información, conozcan o se apoderen de cualquier mensaje de datos. Serán reprimidas con pena privativa de libertad no menor de uno ni mayor de tres años y con sesenta a ciento veinte días multa.

La divulgación o la utilización fraudulenta de la información reservada, los secretos comerciales o industriales que han sido obtenidos por alguna de las formas indicadas en el párrafo anterior será sancionada con pena privativa de libertad no menor de cuatro ni mayor de siete años y con noventa a trescientas días multa.

Si la divulgación o la utilización fraudulenta de los datos o información reservada, los secretos comerciales o industriales, se realiza por la persona o personas a las cuales se les encomendó su custodia o utilización, serán sancionadas con una pena de privativa de libertad no menor de cinco ni mayor ocho años, con cien a trescientos días multa e inhabilitación para desempeñar cargos iguales o similares.

La violación de la reserva al secreto profesional será sancionada de acuerdo a lo dispuesto en el art. 165 del Código Penal.

259 Proyecto de Ley N.º 10079/2003, art. 207-G.- En caso de que una persona o personas, ya sean naturales o jurídicas, recopilaren por medios fraudulentos datos o información nominativa personal para después cederla, publicarla, utilizarla o transferirla a cualquier título sin la automación de su titular o titulares, serán sancionados con pena privativa de libertad no menor de uno ni mayor de tres años y con multa de sesenta a ciento veinte días multa, sin perjuicio de las indemnizaciones correspondientes. Además de la inhabilitación de permanecer en el cargo o continuar con su actividad en el caso de personas naturales, y en el caso de las personas jurídicas se comunicará al Instituto Nacional de Defensa de la Competencia y la Protección de la Propiedad Intelectual (INDECOPI) para que se proceda a su inmediata liquidación.

pues expresamente señala que ostenta una especial protección: "El Congreso debe tener presente que la información es un bien jurídico que debe ser especialmente protegido por el Estado, puesto que de ella y de su administración depende el giro normal de las relaciones comerciales y civiles de la sociedad". En segundo lugar, es uno de los proyectos de ley que describe con mayor detalle la tipificación de las conductas ilícitas. En tercer lugar, se aprecia un sesgo común: pensar que el sujeto activo ostenta características especiales. Así, se dice: "Las personas que cometen los delitos informáticos son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aun cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos". Alejarnos de este tipo de prejuicios nos permitirá aproximarnos e investigar, de mejor forma, la ciberdelincuencia.

Finalmente, en este quinquenio también se propuso la incorporación de este tipo de ilícitos al Código de Justicia Militar Policial:

e. Proyecto de Ley N.º 11346/2004, presentado el 6 de setiembre de 2004 por el congresista Pedro Morales Mansilla. Se propuso incluir tres tipos penales y una circunstancia agravante al Código de Justicia Militar. De esta forma, se sancionaría el acceso ilícito o intrusismo informático[260], la divulgación de información reservada o secretos militares[261] y el atentado contra sistemas informá-

260 Proyecto de Ley N.º 11346/2004, art. S/N.- El militar que ingresa indebidamente a una base de datos, sistema o red de computadoras o cualquier parte de la misma, para interferir, interceptar, acceder o copiar información en tránsito o contenida en una base de datos será reprimida con reclusión militar no menor de un año.

261 Proyecto de Ley N.º 11346/2004, art. S/N.- La divulgación o la utilización fraudulenta de los datos o información reservada y de los secretos militares, realizada por militares a quienes se les encomendó su custodia o utilización, será reprimida con

ticos[262], agravándose la sanción cuando se pusiere en peligro la seguridad nacional[263].

3.3.1.3. Periodo legislativo 2006-2011

En el periodo 2006-2011, se presentaron tres proyectos de ley para crear un cuerpo normativo independiente al CP y especializado en delitos informáticos. Estas tres propuestas se erigen como las primeras en sistematizar el fenómeno delictivo de acuerdo con el bien jurídico prioritariamente protegido. Debido a su extensión, en este punto solo mencionaré la estructura propuesta -analizándose a detalle en el capítulo X de esta publicación-:

a. Proyecto de Ley N.° 1318/2006, presentado el 21 de mayo de 2007 por la Célula Parlamentaria Aprista. Los congresistas propusieron la creación de la *Ley de represión de los delitos informáticos*, que tendría seis capítulos: I. Objeto de la ley. II. Delitos contra los sistemas que utilizan tecnologías de información. III. Delitos informáticos contra la propiedad. IV. Delitos informáticos contra la privacidad de las personas y de las comunicaciones. V. Delitos informáticos contra el orden económico. VI. Disposiciones comunes.

b. Proyecto de Ley N.° 1828/2007, presentado el 31 de octubre de 2007 por el congresista Álvaro Gutiérrez Cueva. El legislador propuso la *Ley que penaliza los delitos informáticos*, norma que estaría

---

pena privativa de libertad no menor de cinco ni mayor de doce años e inhabilitación para desempeñar cargos similares.

262 Proyecto de Ley N.° 11346/2004, art. S/N.- Es responsable de intrusión indebida a los sistemas informáticos, de información o telemáticos, el militar que por cualquier medio o fin, y con el ánimo de apoderarse de la información contenida en dichos sistemas, o para descubrir los secretos militares, o para vulnerar la seguridad militar sin consentimiento o autorización, interfiera, interrumpa, acceda a sistemas de información, conozca o se apodere de cualquier mensaje de datos, será reprimido con pena privativa de libertad no menor de dos ni mayor de cinco años.
La divulgación de los secretos militares que han sido obtenidos por algunas de las formas indicadas en el párrafo anterior será sancionada con pena privativa de libertad no menor de cuatro ni mayor de diez años.

263 Proyecto de Ley N.° 11346/2004, art. S/N.- En el caso de los arts. Anteriores, la pena será privativa de libertad, no menor de ocho ni mayor de quince años, cuando el militar pone en peligro la seguridad nacional.

dividida en siete capítulos: I. Objeto de la ley. II. De los delitos contra la propiedad. III. Daño a datos informáticos. IV. Fraude realizado por medios informáticos. V. Entrega, venta y distribución de medios destinados a cometer delitos previstos en este artículo. VI. Restricción a la prestaciones de servicios de internet. VII. Disposiciones comunes.

c. Proyecto de Ley N.º 3083/2008, presentado el 12 de marzo de 2009 por Juan Carlos Eguren Neuenschwander. Esta propuesta sería actualizada el 11 de agosto del 2011 mediante el proyecto de Ley N.º 00034/2011 por el mismo legislador.

Se propuso crear la *Ley de Delitos Informáticos,* la cual tendría nueve capítulos: I. Generalidades. II. Delitos contra los sistemas de información y Tecnologías de la Información. III. Delitos informáticos contra la intimidad y el secreto de las comunicaciones. IV. Delitos informáticos contra la indemnidad sexual. V. Delitos informáticos contra el patrimonio. VI. Delitos informáticos contra la fe pública. VII. Delitos informáticos contra la propiedad intelectual. VIII. Disposiciones comunes. IX. Disposiciones procesales.

Además, se recibió una propuesta para regular los sistemas informáticos a fin de prevenir la comisión de este tipo de ilícitos:

d. Proyecto de Ley N.º 4279/2010, presentado el 2 de setiembre de 2010 por el legislador Luis Humberto Falla Lamadrid. Propuso la creación de la *Ley especial de delitos informáticos que regula y sanciona a los usuarios infractores de la tecnología de la información y comunicaciones*. Este proyecto es muy interesante, pues es el primero en proponer la adopción del *agente virtual encubierto*[264] *-figura que*

264 Proyecto de Ley N.º 4279/2010, art. 6.- La Policía Nacional para el cumplimiento de su misión y funciones tendrá la facultad de crear personajes virtuales que serán utilizados para ingresar por medio de las comunidades criminales de distintas índoles, pudiendo intercambiar materiales prohibidos en formato digital, con la finalidad de la detección e identificación de los responsables, a otros implicados y/o desbaratar la organización criminal.

sería recogida años más tarde en la LDI, así como la "posesión y manipulación legal de pornografía infantil en archivos digitales"[265].

En lo sustantivo, este proyecto de ley recomendó incorporar nuevas formas delictivas al artículo 207-A CP[266], ampliar los alcances del artículo 207-B CP[267], tipificar la venta indebida de información[268], la obtención indebida de datos o información portable[269], así como la clonación de medios de almacenamiento digital[270].

---

265 Proyecto de Ley N.º 4279/2010, art. 8.- Autorícese a la Policía Nacional la manipulación electrónica y/o magnética de material pornográfico infantil para fines exclusivos del cumplimiento de sus funciones para cuyo efecto implementará un sistema de archivos virtuales magnético o electrónico debidamente autorizado por su propio Comando.

266 Proyecto de Ley N.º 4279/2010, art. 2.- Agréguese al art. 207-A CP, como delito informático, las siguientes figuras:
- El ingreso indebido para alterar, interferir, interceptar o copiar archivos magnéticos, electrónicos y/o datos digitalizados.
- Obtención indebida de claves de usuarios de uso virtual para las comunicaciones y/o transferencias financieras.
- La instalación de software o hardware espías en cualquiera de sus formas si conocimiento del propietario o usuario del equipo.

267 Proyecto de Ley N.º 4279/2010, art. 3.- También será considerado dentro del alcance del art. 207-B, si para la ejecución del ilícito el agente emplea conocimiento técnico de intrusismo y/o cualquier tipo de *software* espía cuando son realizados a distancia.

268 Proyecto de Ley N.º 4279/2010, art. 9.- El que indebidamente comercialice archivos digitales, magnéticos o electrónicos o cualquier otro medio de almacenamiento que ofrece las Tecnologías de la Información y Comunicaciones (TICS) conteniendo data o información confidencial de personas naturales o jurídicas en forma de cartera de clientes o similares, sin conocer su procedencia o sin el consentimiento de aquel a quien le pertenece, sea esta persona natural o jurídica, será reprimido con pena privativa de libertad no menor de dos ni mayor de cuatro años.

269 Proyecto de Ley N.º 4279/2010, art. 10.- El que por cualquier medio no autorizado o indebido obtenga data o información contenida en una tarjeta magnética, electrónica o inteligente o el mismo medio físico, de cuentas activas para transacciones financieras, aunque estas no se hayan consumado, será reprimido con pena privativa de libertad no menor de dos ni mayor de cuatro años. Igual pena será para quien facilite los equipos de copiado o clonación y para quienes posean estos equipos para fines ilícitos.

270 Proyecto de Ley N.º 4279/2010, art. 11.- El que posea algún medio de almacenamiento digital como las tarjetas magnéticas, electrónicas o inteligentes con datos o información de cuentas activas para transacciones financieras, que no le corresponda

3.3.2. Incorporación de nuevos delitos informáticos al Código Penal

Durante la década posterior a la incorporación de los delitos informáticos al CP, el número de estas conductas ilícitas se incrementaron. Así, entre enero del 2000 y diciembre del 2010, se registraron 975 denuncias por delitos informáticos en 27 distritos judiciales, pero solo se formalizaron el 32,3 % de aquellas[271]. De forma paralela, como aquí se explicará, se tipificaron nuevas formas delictivas o precisaron sus alcances para salvaguardar el principio de legalidad en materia penal.

Entre los delitos cuyos alcances se precisaron tenemos la pornografía infantil o distribución de imágenes y videos de explotación sexual infantil (2004), la explotación sexual infantil en el turismo (2004) y la apología al terrorismo (2007). Toda vez que este trabajo se enfoca en los ciberdelitos contra la seguridad informática, se abordarán dos ilícitos conexos: penalización de la clonación o adulteración de terminales de telefonía celular (2006) y elusión de medidas tecnológicas (2008).

3.3.2.1. Penalización de la clonación o adulteración de terminales de telefonía celular (art. 222-A CP), 2006

El 7 de julio de 2006 se publicó la Ley N.º 28774 o *Ley que crea el Registro Nacional de Terminales de Telefonía Celular, establece prohibiciones y sanciona penalmente a quienes alteren y comercialicen celulares de procedencia dudosa*, norma que incorporó el delito bajo análisis al Código Penal:

> **Art. 222-A CP.-** Será reprimido con pena privativa de libertad no menor de dos ni mayor de cinco años, con sesenta a trescientos sesenta y cinco días multa, el que altere, reemplace, duplique o de cualquier modo modifique un número de línea, o de serie electrónico, o de serie mecánico de un terminal celular, de modo tal que pueda ocasionar perjuicio al titular o usuario del mismo, así como a terceros.

---

al medio de almacenamiento que lo porta, aunque estas no hayan sido utilizadas, será reprimido con pena privativa de libertad no menor de dos ni mayor de cuatro años.

271 Observatorio de criminalidad del Ministerio Público. "Delitos informáticos registrados por el Ministerio Público. Enero 2000 – Diciembre 2010". En: *Persecución estratégica del delito.* Año 2. N.º 2, febrero. Lima: Ministerio Público, 2011, p. 8.

Este delito fue incorporado a nuestro ordenamiento, a raíz de un único proyecto de ley, cuya redacción fue aprobada sin ningún tipo de modificación:

- El proyecto de Ley N.º 13855/2005, presentado el 10 de octubre de 2005 por la Célula Parlamentaria Aprista. Si bien no es un ciberdelito, sí me parece oportuno incluirlo por la relación de los dispositivos móviles (instrumento) para la comisión de otros tantos como, por ejemplo, el *vishing*. Esta propuesta normativa resalta que se deben sancionar estas conductas por el riesgo que generan, además, a la privacidad del secreto de las comunicaciones: "Mediante la clonación es posible la utilización del servicio de telefonía móvil sin pago alguno, afectando al titular del equipo. También, mediante la clonación es posible el acceso furtivo a las comunicaciones telefónicas entabladas por el usuario, al duplicarse el número de líneas que identifica al equipo celular. Esto es un riesgo para la privacidad de las comunicaciones, al interceptarse el audio de las mismas".

Este artículo sería modificado el 27 de julio de 2015, por el Poder Ejecutivo, mediante el decreto legislativo N.º 1182 o *Decreto Legislativo que regula el uso de los datos derivados de las telecomunicaciones para la identificación, localización y geolocalización de equipos de comunicación, en la lucha contra la delincuencia y el crimen organizado*. Esta norma también sería conocida como *Ley de la Geolocalización Policial* y sería objeto de diversas críticas[272]:

> **Art. 222-A CP.-** Será reprimido con pena privativa de libertad **no menor de cuatro ni mayor de seis años**, con sesenta a trescientos sesenta y cinco días multa, el que altere, reemplace, duplique o de cualquier modo modifique un número de línea, o de serie electrónico, o de serie mecánico de un terminal celular, **o de IMEI electrónico o físico** de modo tal que pueda ocasionar perjuicio al titular, al usuario del mismo, a terceros o **para ocultar la identidad de los que realizan actos ilícitos.**

272 Estas críticas fueron abordadas en: Elías Puelles, Ricardo. *Decreto Legislativo 1182. Geolocalización y proceso penal. Sacrificios de garantías en favor de una supuesta eficacia investigativa*. Lima: Hiperderecho, 2016. https://hiperderecho.org/wp-content/uploads/2016/05/elias_geolocalizacion_proceso_penal.pdf

Como puede apreciarse, se elevó la sanción mínima y máxima a imponer, se incluyó el código IMEI o *International Mobile System Equipment Identity* como objeto del delito y se adicionó una finalidad: ocultamiento de la identidad de quienes realizan actos ilícitos.

3.3.2.2. Elusión de medidas tecnológicas, productos destinados a la elusión de medidas tecnológicas y servicios destinados a la elusión de medidas tecnológicas (arts. 220-A, 220-B y 220-C CP), 2008

La Ley N.º 29263 del 2 de octubre de 2008 –modificada por la Ley N.º 292316 del 14 de enero de 2009- incorporó estas tres modalidades delictivas propuestas por el Ejecutivo a través del proyecto de Ley N.º 2547/2007 del 30 de junio de 2008, a fin de cumplir con las obligaciones asumidas por el Estado peruano en el artículo 16 del Acuerdo de Promoción Comercial Perú-Estados Unidos[273].

> **Art. 220-A CP.-** El que, con fines de comercialización u otro tipo de ventaja económica, eluda sin autorización cualquier medida tecnológica efectiva que utilicen los productores de fonogramas, artistas, intérpretes o ejecutantes, así como los autores de cualquier obra protegida por derechos de propiedad intelectual, será reprimido con pena privativa de libertad no mayor de dos años y de diez a sesenta días multa.
>
> **Art. 220-B CP.-** El que, con fines de comercialización u otro tipo de ventaja económica, fabrique, importe, distribuya, ofrezca al público, proporcione o de cualquier manera comercialice dispositivos, productos o componentes destinados principalmente a eludir una medida tecnológica que utilicen los productores de fonogramas, artistas intérpretes o ejecutantes, así como los autores de cualquier obra protegida por derechos de propiedad intelectual, será reprimido con pena privativa de libertad no mayor de dos años y de diez a sesenta días-multa.

273 Lamentablemente, la discusión generada a partir de la propuesta de incorporación de estos nuevos delitos al Código Penal fue ínfima. Así, en el debate del 4 de septiembre de 2008, encontramos que al referirse al art. 220-A CP únicamente se señala lo siguiente: "Hay programas que están encriptados, que incluso se pueden bajar del satélite o de Internet por aquel que desarrolla programas para romper esa seguridad puesta por el titular de la propiedad intelectual".

> **Art. 220-C CP.**- El que, con fines de comercialización u otro tipo de ventaja económica, brinde u ofrezca servicios al público destinados principalmente a eludir una medida tecnológica efectiva que utilicen los productores de fonogramas, artistas intérpretes o ejecutantes, así como los autores de cualquier obra protegida por derechos de propiedad intelectual, será reprimido con pena privativa de libertad no mayor de dos años y de diez a sesenta días-multa.

La Ley N.º 29263 también incorporó delitos afines al objeto del presente estudio: (i) art. 220-D CP.- Delitos contra la información sobre gestión de derechos, (ii) art. 220-E CP.- Etiquetas, carátulas y empaques, (iii) art. 220-F CP.- Manuales, licencias u otra documentación o empaques no auténticos relacionados a programas de ordenador.

3.4. TERCER PERIODO: DEL 2013 A DICIEMBRE DE 2023

Entre agosto del 2011 y mediados del 2013, se presentaron nueve proyectos que originaron la promulgación de la Ley N.º 30096 del 22 de octubre de 2013, conocida como Ley de Delitos Informáticos y un proyecto que propuso la incorporación del delito de tráfico ilegal de datos a nuestro ordenamiento penal -ilícito que se encontraría vigente, apenas dos meses, pues fue derogado al promulgarse la LDI-.

3.4.1. Tráfico ilegal de datos (art. 207-D CP), 2013

Trece años después de la incorporación de los delitos informáticos al Código Penal, el legislador creó el delito de Tráfico Ilegal de Datos (art. 207-D CP). Este artículo fue propuesto mediante el proyecto de Ley N.º 2129/2012[274],

274 Proyecto de Ley N.º 2129/2012, art. 2. CP, art. 207-D. Venta ilegal de datos.
El agente que utiliza con la finalidad de comercializar, traficar, vender, promover, favorecer o facilitar, información contenida en una base de datos sobre una persona física, identificada o identificable, sin su autorización, relativa a su origen étnico o racial, o que esté referida a sus características físicas, morales o emocionales, a su vida afectiva, familiar, a su domicilio, números telefónicos, patrimonio, situación financiera, laboral o tributaria, o su estado de salud física o mental, o a su ideología y opiniones políticas, creencias o convicciones religiosas o filosóficas, será reprimido con pena privativa de libertad no menor dos ni mayor de cinco años.

presentado el 13 de abril de 2013 por el congresista Jaime Delgado Zegarra e incorporado mediante la Ley N.º 30076 del 19 de agosto de 2013.

Como se recordará, esta ley fue promulgada con el objeto de combatir la inseguridad ciudadana, razón por la cual se modificaron diversos artículos del Código Penal y se crearon 3 delitos, entre ellos, el delito de tráfico ilegal de datos, pues el legislador consideró que uno de los problemas relacionados a la inseguridad ciudadana se encontraba relacionado con la comercialización indebida de información[275]. Lamentablemente, la redacción de esta norma era tan amplia que podía castigarse incluso las actividades realizadas por las agencias de medios o publicidad a través de las *mailing list*.

> **Art. 207-D CP.-** El que crea, ingresa o utiliza indebidamente una base de datos sobre una persona natural o jurídica, identificada o identificable, para comercializar, traficar, vender, promover, favorecer o facilitar información relativa a cualquier ámbito de la esfera personal, familiar, patrimonial, laboral, financiera u otro de naturaleza análoga, creando o no perjuicio, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años.

3.4.2. Ley N.º 30096 o Ley de Delitos Informáticos, 2013

La última propuesta de modificación legislativa fue remitida por el Poder Ejecutivo el 26 de julio de 2013 y se tituló *Ley de represión de la Cibercriminalidad*. Es la que más similitud guarda con nuestro marco normativo actual, pese a que no alcanzó a ser debatida ni dictaminada por ninguna Comisión del

275 En el proyecto de Ley N.º 2129/2012 del 16 de abril de 2013, presentado por el Congresista Jaime Delgado Zegarra, se señala lo siguiente: "Actualmente uno de los problemas existentes es el de la comercialización indebida de información. En estos lugares, identificados como las zonas comerciales de la Av. Wilson, Polvos Azules, Av. Argentina entre otros no tan recurridos, cualquier persona puede adquirir a precios asequibles bases de datos completas empleadas para la sistematización de datos por sectores de la industria o el comercio. Lo preocupante es que más allá de la aparente impunidad con que los traficantes pueden realizar las transacciones comerciales ilegales de venta de bases de datos, la vulnerabilidad de nuestra información queda reflejada en lo fácil que es obtener esta base de datos de primera fuente para su posterior venta ilegal".

Legislativo antes de ser discutida en el Pleno[276]. Es más, este proyecto fue modificado en menos de seis horas y aprobado con un texto sustitutorio que no fue puesto a debate a la sociedad civil, lo que generó gran malestar y preocupación a nivel nacional debido a la ambigüedad de algunas expresiones.

a. Proyecto de Ley N.º 34/2011, del 11 de agosto de 2011, presentado por Juan Carlos Eguren Neuenschwander. Esta iniciativa propuso un cuerpo normativo independiente por el nivel de especialidad que tiene la informática y la posibilidad de incluir disposiciones procesales para facilitar su investigación. La Ley de Delitos Informáticos adoptó la estructura propuesta en este proyecto.

   El legislador era consciente que no todos los delitos cometidos a través de las TICs requerían ser incluidos en la legislación especial, sino aquellos que por su nivel de sofisticación requerían un tratamiento diferenciado, tal y como lo reflejó en su exposición de motivos:

> La segunda decisión de técnica legislativa que se ha tornado es no regular todos los delitos informáticos en la ley especial, sino solamente aquellas conductas que no puedan reprimirse adecuadamente con los tipos penales que contiene el actual Código Penal. En este sentido, la ley no prevé sanciones para cualquier forma de ataque a bienes jurídicos por medios informáticos, sino que se limita a los casos que, por sus particularidades, requieren una tipificación especial. En este sentido, no se prevé, por ejemplo, delitos contra el honor ni actos de incitación a la discriminación cometidos por medios informáticos, pues en estos casos los tipos penales existentes en el Código Penal resultan idóneos para repri-

276 Morachimo Rodríguez, Miguel. "Deconstruyendo la Ley de delitos informáticos". En: *Gaceta Constitucional* 71, Lima: 2013, p. 346. De acuerdo a este autor, también debe tenerse en cuenta que habrían existido presiones externas para su aprobación, ya que "el otro antecedente directo de la Ley de Delitos Informáticos es la reunión de técnicos de la Conferencia de Ministros de Justicia de Iberoamérica (COMJIB), que se llevó a cabo en Lima a fines de junio [...]. Se sabe que en la última reunión de Lima se avanzó sobre la redacción de un convenio sobre la ciberdelincuencia para la región, que ha pasado a evaluación y espera ser firmado por todos los países antes de que termine el 2013" (Morachimo Rodríguez, "Deconstruyendo la Ley de delitos informáticos", cit., p. 347).

mir estas conductas. Esta ley penal se ocupa, más bien, de perfilar los delitos informáticos que afectan a los sistemas informáticos (la informática como objeto) y los supuestos de uso de sistemas informáticos para lesionar otros bienes jurídicos que no puedan reprimirse satisfactoriamente con los tipos penales contenidos en el Código Penal (la informática como medio).

b. Proyecto de Ley N.° 307/2011, del 05 de octubre de 2011, presentado por Octavio Salazar Miranda. El congresista también planteó la creación de un ordenamiento especializado bajo el nombre de *Ley especial sobre delitos cometidos con el uso de las Tecnologías de la Información y Comunicación*. Así, en lo sustantivo planteó la tipificación de los siguientes delitos: Comercialización o difusión de base de datos, prestación de servicios para sabotaje informático y posesión de equipos de sabotaje informático. Además, sugirió la adopción de técnicas de investigación y de aseguramiento de la prueba digital -algunas sí fueron recogidas en la Ley de Delitos informáticos-: codificación de pornografía infantil, agente encubierto en el ciberespacio, acceso a información de los protocolos de internet, recojo y conservación de bienes usados para cometer el delito y uso de las especies incautadas.

c. Proyecto de Ley N.° 1136/2011, del 17 de mayo de 2012, presentado por Tomás Zamudio Briceño. A diferencia de las dos propuestas precedentes, se propuso modificar el artículo 207-C CP y adicionar el 207-D. El primero proponía sancionar el delito de suplantación de identidad, denominándolo *robo de identidad virtual*; el segundo, crear circunstancias agravantes que permitan incrementar la pena hasta los siete años de cárcel.

d. Proyecto de Ley N.° 1257/2011, del 14 de junio de 2012, presentado también por Tomás Zamudio Briceño. Esta iniciativa recomendó adicionar dos artículos al Código Penal: delito de inviolabilidad del secreto de las comunicaciones (art. 161-A CP) y responsabilidad de los concesionarios de servicios públicos (art. 161-B CP). Además, sugirió modificar el delito de tenencia ilegal de partes y equipos de interceptación telefónica (art. 162-A CP).

Esta propuesta se presenta después que los medios de comunicación informaran las interceptaciones telefónicas que involucraron a funcionarios de la Municipalidad Provincial del Callao, el Gobierno Regional del Callao y el movimiento político Chim Pun Callao. En este sentido, luego de recordar el caso Business Track, el legislador señala que estas modalidades delictivas no fueron contempladas en el Código Penal de 1991, ya que la tecnología no había avanzado tan vertiginosamente.

e. Proyecto de Ley N.º 2112/2011, del 12 de abril de 2012, presentado por Renzo Andrés Reggiardo Barreto. Esta propuesta normativa recomendó, de un lado, modificar los delitos de receptación (art. 194 CP), distribución no autorizada de señal de cable (art. 194-A CP), estafa (art. 196 CP) y penalización de la clonación o adulteración de terminales de telefonía (art. 222-A CP) y, de otro, incorporar cuatro delitos al ordenamiento penal: hurto de señal de internet o cable (art. 185-A CP), fraude informático (art. 196-A CP), fraude a los servicios de telefonía (art. 196-B CP) y servicios de telecomunicaciones no autorizadas administrativamente (art. 243-D CP).

   El autor de este proyecto destacó la ausencia de tipos penales específicos que desincentiven modernas conductas delictivas cometidas por los cibercriminales. Así, en palabras de su autor:

> El Perú se está convirtiendo en un paraíso para los cibercriminales debido a la falta de una adecuada legislación. Ello deriva en que miles de peruanos se vean afectado por la comisión de delitos informáticos. Así, se plantea penalizar conductas delictivas que son desarrolladas a través de las telecomunicaciones y que no estaban contempladas en la legislación penal debido a los avances tecnológicos. A través de la penalización de la figura de fraude informático, se buscará que delitos como la ciberestafa, clonación de tarjetas, *phishing*, entre otros no queden impunes.

f. Proyecto de Ley N.º 2129/2011, del 12 de abril de 2012, presentado por Jaime Delgado Zegarra. Bajo el nombre de *Ley que sanciona la venta ilegal de base de datos y datos personales de usuarios*

y consumidores, el legislador propuso incorporar el artículo 207-D al Código Penal.

En la exposición de motivos, el legislador resalta la facilidad con la que se pueden adquirir bases de datos "en las zonas comerciales de la Av. Wilson, Polvos Azules, Av. Argentina, entre otros no tan concurridos" y la ausencia de un tipo penal que lo sancione. Así, remarca que "el peligro para la privacidad del individuo no radica en que se acumule información sobre él, sino, más bien, en que pierda la capacidad de disposición sobre ella y respecto a quién, y con qué objeto se transmite aquella información".

He de indicar que esta iniciativa legislativa fue exitosa, pues este delito fue incorporado al Código Penal, mediante Ley N.º 30076 del 19 de agosto del 2013. Sin embargo, fue derogado el 22 de octubre del mismo año -es decir, dos meses después- al promulgarse la Ley de Delitos Informáticos.

g. Proyecto de Ley N.º 2520/2011, del 26 de julio de 2013, presentado por el presidente Ollanta Humala Tasso. Como he mencionado anteriormente, esta propuesta es la que más influencia tuvo en la actual redacción de los tipos penales recogidos en la LDI. Así, pese a que no propuso una legislación especial, sino la incorporación de un nuevo Título al Código Penal, los delitos sugeridos fueron los que, finalmente, se adoptaron. La influencia del Convenio de Budapest es palpable y, si el lector revisa su exposición de motivos, apreciará que textualmente lo menciona:

> En cuanto al Tratado de Budapest (2001), diversas consideraciones y convicciones del Consejo de Europa determinaron la necesidad de establecer una política penal frente a la cibercriminalidad expansiva. Dos de sus pilares discursivos son una adecuada legislación y la mejora de la cooperación internacional. De este modo, el Tratado se desarrolla en la tipificación de conductas a nivel sustantivo, mecanismos procesales correspondientes, y estrategias de participación interinstitucional referidas a la investigación y medidas preventivas[277].

277 Recomiendo al lector revisar la exposición de motivos, pues, en sus 19 páginas, desarrolla incidencia delictiva, la expansión de la cibercriminalidad, el desarrollo de la

A continuación, detallo los tipos penales y cómo pensaban ser regulados: acceso ilícito (art. 208-A CP), atentados a la integridad de datos informáticos (art. 208-B CP), atentados a la integridad de sistemas informáticos (art. 208-C CP), abuso de mecanismos y dispositivos informáticos (art. 208-D CP) y formas agravadas (art. 208-E CP), interceptación de datos informáticos (art. 162-A CP), proposiciones a niños con fines sexuales por medios tecnológicos (art. 183-B CP), fraude informático (art. 197-A CP) y suplantación de identidad (art. 438-A CP). Además, propuso modificar dos delitos ya previstos en el ordenamiento: pornografía infantil (art. 183-A CP) y discriminación (art. 323 CP).

Finalmente, debo destacar que este proyecto de ley recoge las disposiciones complementarias finales que serían acogidas en la LDI: (i) convenios multilaterales, (ii) terminología, (iii) coordinación interinstitucional de la Policía Nacional con el Ministerio Público, (iv) cooperación operativa, (v) capacitación, (vi) medidas de seguridad y (vii) buenas prácticas.

3.4.3. Modificación de la Ley N.° 30096 o Ley de Delitos Informáticos, 2014

Pocas semanas después de la promulgación de la LDI, se propusieron cinco nuevos proyectos de ley que buscaban precisar la tipificación de los nuevos delitos al amparo de estándares internacionales en materia de cibercriminalidad:

a. Proyecto de Ley N.° 2991/2013, del 25 de noviembre de 2013, presentado por Juan Carlos Eguren Neuenschwander. Entre otros aspectos, se propuso incorporar las expresiones *deliberada* e *ilegítimamente* a los delitos de acceso ilícito (art. 2 LDI), atentado contra la integridad de datos y sistemas informáticos (arts. 3 y 4 LDI), interceptación de datos informáticos (art. 7 LDI), fraude informático (art. 8 LDI) y abuso de mecanismos y dispositivos (art. 10 LDI).

   De manera errónea, este proyecto de ley afirma que nuestra legislación necesitaba la incorporación que, finalmente se aceptó, para

cibercriminalidad en América Latina y en Perú y los diferentes problemas normativos que la propuesta legislativa busca solucionar.

cumplir con los estándares legislativos propuestos en el Convenio de Budapest.

b. Proyecto de Ley N.º 2999/2013, del 27 de noviembre de 2013, presentado por Mauricio Mulder Bedoya. Recoge la misma propuesta que el proyecto antes mencionado: agregar las expresiones *deliberada* e *ilegítimamente* a los arts. 2, 3, 4, 7, 8 y 10 LDI.

   Pese a que la exposición de motivos detalla que este proyecto busca precisar las modalidades delictivas de la LDI, propuso modificar el delito de suplantación de identidad por una fórmula extremadamente genérica y que hubiese dejado sin protección a las personas jurídicas: "El que suplanta la identidad de una persona natural será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años". Esta propuesta felizmente no prosperó.

c. Proyecto de Ley N.º 3048/2013, del 5 de diciembre de 2013, presentado por José Luna Gálvez. Se propuso incorporar un verbo rector al delito de interferencia telefónica (art. 162 CP), modificado previamente por la LDI. Además, incluir una nueva forma agravada.

   El proyecto de ley recoge la sugerencia planteada en el *Informe sobre legislación comparada referida al tema de interceptación telefónica*, elaborado por el Centro de Investigación, Análisis Temático e Investigación del Congreso de la República.

d. Proyecto de Ley N.º 3105/2013, del 18 de diciembre de 2013, presentado por Carmen Omonte Durand. Si bien la iniciativa recomendó modificar los arts. 3, 7 y 10 LDI, debo destacar que fue esta propuesta normativa la que incorporó el verbo *dañar* al delito de atentado a la integridad de datos informáticos.

Estos proyectos se debatieron en la Comisión Permanente el 12 de febrero del 2014, logrando su exoneración de la doble votación y la promulgación de la Ley N.º 30171 del 10 de marzo de 2014.

De modo general, he de indicar que la LDI está estructurada actualmente de la siguiente manera, en lo que a ciberdelitos contra la seguridad informática se refiere:

Ley N.° 30096 o Ley de Delitos Informáticos		
Sección	**Denominación**	**Artículos comprendidos**
Capítulo II	Delitos contra datos y sistemas informáticos	Art. 2.- Acceso ilícito Art. 3.- Atentado a la integridad de datos informáticos Art. 4.- Atentado contra la integridad de sistemas informáticos
Capítulo IV	Delitos informáticos contra la intimidad y el secreto de las comunicaciones	~~Art. 6.- Tráfico ilegal de datos~~[278] Art. 7.- Interceptación de datos informáticos
Capítulo VII	Disposiciones comunes	Art. 10.- Abuso de mecanismos y dispositivos informáticos Art. 11.- Agravantes Art. 12.- Exención de responsabilidad

Cuadro 11. Cuadro resumen de los ciberdelitos contra la seguridad informática recogidos en la LDI. Elaboración propia.

Antes de finalizar este apartado, debo indicar que el 13 de noviembre del 2014 se recibió el proyecto de Ley N.° 3980/2014, propuesto por la congresista Martha Chávez Cossio, por el cual intentó modificar tanto el objeto de la Ley de Delitos Informáticos (art. 1 LDI) para precisar que se busca proteger "el derecho a la propiedad, la protección de los datos personales y la intimidad de las personas contenidos en" los sistemas y datos informáticos, como el delito de abuso de mecanismos y dispositivos informáticos (art. 10 LDI). Esta propuesta fue rechazada.

3.4.4. Periodo Legislativo 2016-2021

En este periodo legislativo se recibieron cinco propuestas normativas relacionadas a la cibercriminalidad.

a. Proyecto de Ley N.° 5226/2020, del 15 de mayo de 2020, presentado por María Martina Gallardo Becerra. Esta iniciativa postuló incorporar una nueva agravante al artículo 11 LDI, "cuando el agente comete el delito durante el Estado de Emergencia Nacional".

b. Proyecto de Ley N.° 5630/2020, del 25 de junio de 2020, presentado por Robertina Santillana Paredes. La legisladora propuso derogar la LDI y crear un nuevo marco normativo especializado,

278 Artículo actualmente eliminado de la LDI, mediante la única disposición complementaria derogatoria de la Ley N.° 30171, publicada el 10 de marzo de 2014.

titulado como *Ley de Seguridad Informática y Represion de Delitos Informáticos.*

Debo destacar que esta propuesta recoge, entre otros, dos capítulos muy interesantes: (i) procedimientos de investigación criminal de los delitos informáticos, en el que postula un marco especial en torno a la intervención de las comunicaciones, el levantamiento del secreto bancario, reserva tributaria y bursátil, la incautación de bienes materia del delito, el bloqueo de dominios, la audiencia judicial de reexamen y la colaboración eficaz. (ii) Delitos informáticos, en el que propone los siguientes tipos penales: Intrusismo informático, perturbación informática, interceptación de datos informáticos, suplantación de identidad, creación de falsa identidad, pornografía infantil, fraude informático y abuso de mecanismos y dispositivos informáticos.

Si bien los proyectos de ley descritos no fueron aprobados, demuestran la preocupación actual en torno a la ciberdelincuencia y el rol del Poder Legislativo en el fortalecimiento de su enfrentamiento, en aras de sancionar nuevas modalidades delictivas.

3.4.5. Adhesión del Perú al Convenio de Budapest, 2019

En el capítulo anterior, resalté la importancia del Convenio de Budapest o Convenio sobre la Ciberdelincuencia. En este punto, he de indicar que Perú se adhirió al citado Convenio mediante Resolución Legislativa N.º 30913, del 12 de febrero del 2019, acto ratificado a través del Decreto Supremo N.º 010-2019-RE, del 9 de marzo. Así, entró en vigor el 1 de diciembre de ese año.

3.4.5.1. Declaraciones del Perú frente al Convenio de Budapest

Es importante precisar que Perú efectuó cuatro declaraciones -tres sobre delitos y uno sobre un procedimiento relativo a la asistencia mutua entre estados-, que fue publicado en la separata especial del diario *El Peruano*, el 22 de setiembre de 2019:

a. Respecto al delito de **acceso ilícito**, Perú declaró lo siguiente: "De conformidad con lo dispuesto en el art. 2 del Convenio sobre la Ciberdelincuencia, la República del Perú declara que su legisla-

ción exige que el delito de acceso ilícito se cometa infringiendo medidas de seguridad".

b. Respecto al delito de **interceptación ilícita**, se declaró lo siguiente: "De conformidad con lo dispuesto en el art. 3 del Convenio sobre la Ciberdelincuencia, la República del Perú declara que su legislación exige que el delito de interceptación ilícita se cometa con intención delictiva y que dicho delito puede cometerse en relación con un sistema informático conectado a otro sistema informático".

c. Respecto al delito de **falsificación informática**, Perú declaró lo siguiente: "De conformidad con lo dispuesto en el art. 7 del Convenio sobre la Ciberdelincuencia, la República del Perú declara que podrá exigir que exista una intención fraudulenta o delictiva similar, conforme a lo establecido en su derecho interno, para que las conductas descritas en dicho art. generen responsabilidad penal".

d. Respecto a los **procedimientos relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables**, se declaró lo siguiente: "De conformidad con lo establecido en el art. 27, numeral 9, literal e) del Convenio sobre la Ciberdelincuencia, la República del Perú declara que, en aras de la eficacia, las solicitudes efectuadas en virtud de lo dispuesto en el numeral 9 del Convenio deberán dirigirse a su autoridad central".

3.4.5.2. Reservas del Perú frente al Convenio de Budapest

Además, nuestro país realizó tres reservas -dos relacionadas a delitos y una sobre conservación rápida de datos informáticos de almacenamiento-:

a. Respecto al delito de **abuso de dispositivos**, el texto de reserva es el siguiente: "De conformidad con lo dispuesto en el párrafo 3 del art. 6 del Convenio sobre la Ciberdelincuencia, la República del Perú se reserva el derecho de no aplicar el art. 6, párrafo 1, literal b del Convenio".

b. Respecto a los delitos relacionados con la **pornografía infantil**, el texto de reserva es el siguiente: "De conformidad con el nu-

meral 4 del art. 9º del Convenio sobre la Ciberdelincuencia, la República del Perú considera que el bien jurídico tutelado en el derecho interno con respecto a la pornografía infantil es la libertad y/o indemnidad sexual de un menor, por lo que formula una reserva a los apartados b) y c) del citado numeral, debido a que las conductas contempladas en dichas disposiciones no involucran la participación de un menor de edad".

c. Respecto a la **conservación rápida de datos informáticos almacenados**, el texto de reserva es el siguiente: "Conforme al numeral 4 del art. 29 del Convenio sobre la Ciberdelincuencia, la República del Perú se reserva el derecho a denegar la solicitud de conservación en virtud de dicho art. en el caso que tenga motivos para creer que, en el momento de la revelación de los datos, no se cumplirá con la condición de la doble tipificación penal".

3.5. CUARTO PERIODO: DE DICIEMBRE DEL 2023 A LA ACTUALIDAD

3.5.1. Modificaciones a la LDI: Decretos Legislativos 1591 y 1614, 2023

Mediante Ley N.º 31880[279], se delegó en el Poder Ejecutivo la facultad de legislar en materia de seguridad ciudadana, gestión del riesgo de desastres, infraestructura social, calidad de proyectos y meritocracia por el plazo de 90 días. Es así que, en diciembre del 2023, como parte de un paquete de reformas sustantivas y procesales, el Ejecutivo modificó la LDI. De este modo, se publicaron dos decretos legislativos que modificaron cuatro delitos y una norma procesal recogida en el cuerpo normativo en referencia:

a. **Decreto Legislativo N.º 1591** del 12 de diciembre del 2023: modificó los delitos de *grooming* o proposiciones a niños, niñas y

279 **Ley N.º 31880, art. 2.** ***Materia de delegación de facultades.***
2.1 En materia de seguridad ciudadana [...]
2.1.3 Lucha contra la delincuencia y el crimen organizado [...]
b) Fortalecer la lucha contra la extorsión, la estafa, el fraude y otros delitos a través de la aprobación de medidas y normas modificatorias al marco normativo, con la intención de prevenir y hacer frente a la ciberdelincuencia, en estricto respeto a los derechos fundamentales garantizados por la Constitución Política del Perú y los principios de igualdad ante la ley, razonabilidad y proporcionalidad.

adolescentes con fines sexuales (art. 5 LDI) y de suplantación de identidad (art. 9 LDI), así como la figura de agente encubierto en delitos informáticos (segunda disposición complementaria final LDI).

b. **Decreto Legislativo N.º 1614** del 20 de diciembre del 2023: modificó los delitos de acceso ilícito (art. 2 LDI) y fraude informático (art. 8 LDI).

Toda vez que esta publicación se ocupa de los ciberdelitos contra la seguridad informática, en estas líneas mencionaré únicamente los motivos que originaron la modificación del delito de acceso ilícito. Así, en la Exposición de Motivos del Decreto Legislativo N.º 1614 se indica lo siguiente:

> **6.2. Análisis del estado actual de la situación fáctica que se pretende modificar**
>
> Según los últimos reportes periodísticos, se demuestra la facilidad que tienen determinadas personas para ingresar y modificar denuncias en el sistema de seguridad de la Policía Nacional del Perú. Es así que un reportero de un determinado medio periodístico se percató de que mediante la red social Telegram ha advertido una suerte de bandas criminales cibernéticas que operan para realizar, por ejemplo, denuncias públicas, requisitorias, hackeo de whatsapp, deudas bancarias, entre otros servicios ilícitos, ofreciendo sus servicios por 45.00 soles para colocar, por ejemplo, una denuncia policial a una persona por robo agravado a mano armada.
>
> Del mismo modo, la página web del Indeci fue reportada como maliciosa por un proveedor de seguridad. Un experto especialista de ESET Perú señaló que "Esto quiere decir que ciberdelincuentes tuvieron acceso al servidor o a la página web de la institución. ¿Cómo han podido tener acceso a esto? Probablemente haya podido vulnerar cierta parte de la página del Indeci, haber colgado su *malware* dentro del contenedor de la página, de tal manera que cualquier persona que intente ingresar tiene la posibilidad de descargar este *script* en su equipo".
>
> Ante el incremento de los delitos de cibercriminalidad, por precisamente vulnerar los sistemas de seguridad, se propone modificar el artículo 2 de la Ley N.º 30096, incorporando como agravante el supuesto del agente que accede deliberada e ilegítimamente, en todo o en

> parte, al sistema informático vulnerando las medidas de seguridad establecidas para impedirlo, ello con la finalidad de reprimir penalmente con mayor intensidad a aquellas personas que vulneran las medidas de seguridad cuando una determinada institución estatal o empresa privada, cuente con tal.
>
> En caso de que la mencionada institución o empresa no cuente con las medidas de seguridad antes señaladas y aun así el agente acceda deliberada e ilegítimamente al sistema informático, incluso excediéndose o extralimitándose en lo autorizado, nos encontraríamos en el primer párrafo del artículo 2 de la Ley N.º 30096, que regula el acceso ilícito.

La norma aludida se actualizó en los siguientes términos:

> **Art. 2 LDI.-** El que deliberada e ilegítimamente accede a todo o en parte de un sistema informático, o se excede en lo autorizado, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa.
>
> Si el agente accede deliberada e ilegítimamente, en todo o en parte, al sistema informático vulnerando las medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa.

Si bien el delito de acceso ilícito será analizado en el capítulo correspondiente, se presentan algunos apuntes sobre esta modificación: (1) el legislador mantiene los elementos *deliberada* e *ilegítimamente*, (2) el primer párrafo no exige la ruptura de medidas de seguridad, (3) no se establece alguna finalidad adicional, es decir, este delito se mantiene como uno de mero intrusismo, (4) el segundo párrafo contempla un supuesto agravado, esto es, el acceso ilegal con vulneración de medidas de seguridad.

3.5.2. Incorporación de nuevos delitos a la LDI: Decreto Legislativo 1625 y Ley 32183, 2024

Si bien los dos delitos que, a continuación, comentaré no son delitos contra la seguridad informática, su importancia exige que haga una breve mención a estos:

El 8 de agosto, mediante el Decreto Legislativo N.° 1625, se tipificó el delito de **chantaje sexual con materiales elaborados o modificados por medios tecnológicos o digitales (art. 5-A)**, incluyéndolo a la Ley de Delitos Informáticos. A través de las redes, lamentablemente, muchos delincuentes amenazan o intimidan a sus víctimas con la difusión de imágenes de contenido sexual, sin importarles que sean verídicas o adulteradas. ¿Qué exigen a cambio? Mantener algún tipo de encuentro o contacto sexual. Este *chantaje* se castiga con dos a cuatros años de pena privativa de libertad. La pena será de tres a cinco en algunos casos especiales. Por ejemplo, cuando la víctima es menor de edad o hayan tenido algún tipo de relación previa.

El 11 de diciembre, de conformidad con el artículo 2 de la Ley N.° 32183[280], se incorporó el delito de **préstamo informático extorsivo (art. 8-A)** a nuestro ordenamiento. Pese a que no era necesario, pues dicha modalidad ya se castigaba como un tipo de extorsión, el legislador consideró oportuno crear un nuevo delito y reprimirlo con pena privativa de libertad que oscila entre ocho (8) y quince (15) años. Este delito surge como respuesta a los denominados *préstamos gota a gota* -que aumentaron de forma alarmante estos dos últimos años-.

3.5.3. Suscripción del Segundo Protocolo Adicional al Convenio sobre la Ciberdelincuencia, 2024

El 12 de diciembre de 2024, Perú suscribió el Segundo Protocolo Adicional al Convenio sobre la Ciberdelincuencia durante la 31 Sesión Plenaria del Comité. El embajador Ruiz Rosas, en representación de nuestro país, firmó el documento en virtud de la Resolución Suprema N.° 211-2024-RE.

El segundo protocolo está referido a la cooperación reforzada y la divulgación de pruebas electrónicas, siendo su principal objetivo mejorar la comunicación entre los estados y el sector privado para fortalecer el aseguramiento de la prueba digital en el marco de las investigaciones criminales:

> Reconociendo la necesidad de una mayor y más eficaz cooperación entre los Estados y el sector privado, y que en este contexto es necesaria una mayor claridad o seguridad jurídica para los proveedores de servi-

280 Ley que modifica el Código Penal, Decreto Legislativo 635, para incorporar la modalidad de préstamos extorsivos en el tipo penal de extorsión.

> cios y otras entidades en relación con las circunstancias en que pueden responder a las solicitudes directas de las autoridades de justicia penal de otras Partes para la divulgación de datos electrónicos;
>
> Por consiguiente, con el fin de seguir reforzando la cooperación en materia de ciberdelincuencia y la obtención de pruebas en forma electrónica de cualquier delito penal a efectos de investigaciones o procedimientos penales específicos mediante instrumentos adicionales relativos a una asistencia mutua más eficaz y otras formas de cooperación entre las autoridades competentes; la cooperación en situaciones de emergencia, y la cooperación directa entre las autoridades competentes y los proveedores de servicio y otras entidades que posean o controlen la información pertinente [...][281]

3.5.4. Propuesta legislativa, 2024

Concluyo este capítulo destacando la única iniciativa legislativa presentada en el período 2021-2026 que aborda los ciberdelitos contra la seguridad informática: el proyecto de Ley N.º 9443/2024-CR, propuesto el 6 de noviembre de 2024 por el congresista Esdras Medina Minaya, del grupo parlamentario Renovación Popular.

En este proyecto, se analiza el incremento de la ciberdelincuencia en el Perú, tomando como referencia las estadísticas presentadas en el informe de la Defensoría del Pueblo, *La ciberdelincuencia en el Perú: Estrategias y retos del Estado*, de mayo de 2023. Este documento evidencia la creciente sofisticación de los delitos informáticos y los desafíos que enfrenta el Estado para combatirlos. A partir de estos datos, se busca no solo comprender la magnitud del problema, sino también evaluar la eficacia de las estrategias actuales y proponer nuevas acciones para fortalecer la seguridad digital en el país:

> Año 2018: 3031 denuncias
> Año 2019: 7814 denuncias
> Año 2020: 9787 denuncias
> Año 2021: 12 827 denuncias

281 Preámbulo del Segundo Protocolo adicional al Convenio sobre la Ciberdelincuencia, relativo a la cooperación reforzada y la divulgación de pruebas electrónicas.

De este modo, el proyecto de ley propone modificar los delitos de acceso ilícito (art. 2 LDI)[282] y atentado contra la integridad de los sistemas informáticos (art. 4 LDI)[283]. A marzo del 2025, continuaba en la Comisión de Justicia y Derechos Humanos del Congreso de la República.

3.6. CONCLUSIONES DEL CAPÍTULO

- El Código Penal (1991) recogió el delito de hurto telemático como figura agravada, el cual sancionaba tres modalidades de ejecución: utilización de sistemas de transferencia electrónica de fondos, utilización de sistemas telemáticos y violación del empleo de claves secretas. Tres años después se incrementaron las penas.
- La incorporación de los delitos informáticos al Código Penal (2000) fue una respuesta adecuada, pero no suficiente. Así, se recogieron algunas figuras iniciales y básicas, pero, al ubicarse en el título de delitos contra el patrimonio, generó problemas en la identificación del bien jurídico protegido.
- En la década siguiente, se incorporaron nuevas modalidades delictivas a tipos penales clásicos, pues las Tecnologías de la Información y Comunicación facilitaban su comisión: distribución de imágenes y videos de abuso sexual infantil, explotación sexual in-

282 LDI, art. 2.- *Acceso ilícito*
El que deliberada e ilegítimamente accede a todo o en parte de un sistema informático, o se excede en lo autorizado, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa.
Si el agente accede deliberada e ilegítimamente, en todo o en parte, al sistema informático vulnerando las medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa.
Será reprimido con la misma pena el que accede a un sistema informático con el ánimo de apoderarse, divulgar o utilizar la información contenida en el sistema informático.

283 LDI, Art. 4.- *Atentado a la integridad de sistemas informáticos*
El que deliberada e ilegítimamente obstaculice o impida el normal funcionamiento, total o parcialmente, de un sistema informático, a través de la introducción, transmisión, daño, deterioro, alteración o supresión de los datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa.

fantil en el turismo, apología al terrorismo, entre otros. Las exposiciones de motivos, tanto de los proyectos de ley aprobados como rechazados, evidencian la preocupación de un fenómeno criminal que estaba en auge y proliferación.

- La Ley N.º 30096 o Ley de Delitos Informáticos (2013) estableció un cuerpo normativo especializado en el tratamiento de la ciberdelincuencia, siguiendo diversas recomendaciones propuestas en el Convenio sobre la Ciberdelincuencia o Convenio de Budapest. Este marco normativo incluyó dos delitos ajenos al citado Convenio, pero necesarios: el *child grooming* virtual y la suplantación de identidad.
- La Ley N.º 30171 (2014) modificó los delitos de acceso ilícito, atentados contra la integridad de datos y sistemas informáticos, interceptación de datos, fraude informático y abuso de mecanismos y dispositivos, incorporando dos elementos que generan dificultades de interpretación y aplicación práctica: *deliberada* e *ilegítima*. Los promotores del cambio justificaron esta inclusión en los estándares legislativos propuestos en el Convenio de Budapest; sin embargo, no era una exigencia sino una recomendación que cada Estado debía evaluar. En el caso peruano, estos elementos no son necesarios.
- La adhesión de Perú al Convenio sobre la Ciberdelincuencia (2019) y la suscripción del Segundo Protocolo Adicional al Convenio de Budapest (2024) marcan dos hitos históricos, pero no representan el final de nuestro viaje, sino solo un paso -aunque uno muy importante- en la lucha contra este fenómeno delictivo.

CAPÍTULO 4

LA LEY DE DELITOS INFORMÁTICOS: CUESTIONES PRELIMINARES



* La ilustración de la página anterior corresponde a una adaptación de *Neptuno*, de Luca Giordano. Para su elaboración, se empleó una de las herramientas de generación de imágenes de la empresa OpenAI.

CAPÍTULO 4

LA LEY DE DELITOS INFORMÁTICOS: CUESTIONES PRELIMINARES

Sumario: 4.1. Introducción. 4.2. Funciones preventivas y retributivas de la LDI. 4.3. Sistemas y datos informáticos. 4.4. El uso de las TIC como medio comisivo. 4.5. Bienes jurídicos protegidos en la LDI. 4.6. La seguridad informática como bien jurídico protegido. 4.7. Elementos de la seguridad informática y actividad delictiva. 4.8. Actuación deliberada e ilegítima. 4.9. Ser *hacker* no significa ser ciberdelincuente. 4.10. Conclusiones del capítulo.

> [Los términos] *hackers* y *atacantes* no son términos intercambiables que signifiquen lo mismo, es decir, actores maliciosos. Ambos se sirven de habilidades similares, pero sus objetivos son radicalmente diferentes.
>
> Un *hacker* es un profesional de seguridad que investiga y explora de manera proactiva las vulnerabilidades de una organización, con el objetivo de identificarlas antes de que un atacante pueda explotarlas con fines maliciosos [...]. Por el contrario, los atacantes investigan la red y los sistemas de una víctima prevista en busca de vulnerabilidades que se pueden explotar, con el objetivo de obtener ganancias monetarias o para extraer datos valiosos o confidenciales.
>
> En definitiva, los *hackers* sirven para protegerse y son aliados, mientras que los atacantes son todo lo contrario.
>
> Chloé Messdaghi[284]

284 Messdaghi, Chloé. "Cuatro aspectos importantes de ciberseguridad". En: Morillo, Christina (ed.). *97 cosas que todo profesional de la seguridad informática debería saber.* Madrid: Grupo Anaya, 2022, p. 47.

4.1. INTRODUCCIÓN

A diferencia de los países que modificaron diversos artículos de su Código Penal o que incorporaron otros tantos para incluir los ciberdelitos[285], siguiendo la propuesta planteada en el proyecto de Ley N.º 34/2011, Perú optó por agruparlos en una ley especial: la Ley de Delitos Informáticos publicada el 22 de octubre de 2013. Esta técnica legislativa no solo es adecuada, sino que, además, reconoce la trascendencia de este fenómeno delictivo, al establecer en el primer artículo su objeto y finalidad:

> **Art. 1 LDI.-** La presente Ley tiene por objeto prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros

285 En algunas legislaciones, los ataques contra los datos y sistemas informáticos se encuentran regulados en el capítulo de delitos contra el patrimonio, sin embargo, cada vez son más los autores que cuestionan esta opción legislativa. "A efectos expositivos, hemos dedicado un capítulo independiente a esta categoría delictiva teniendo en cuenta que el propio legislador ha considerado como bien jurídico protegido aquí no solamente derechos materiales como sucede en la configuración tradicional del delitos de daños, sino la información contenida en sistemas informáticos propiamente dicha, con lo que se hace difícil, cuanto menos, la reconducción del bien jurídico protegido en esta modalidad típica a una simple manifestación de la propiedad privada. Piénsese, por ejemplo, en los metadatos de las comunicaciones electrónicas o del Internet de las Cosas. Incluso cabría ir más allá, ya que la reforma de 2015 tutela el funcionamiento de infraestructuras críticas públicas o privadas. Por todo ello, se produce una despatrimonilización de la concepción tradicional que debería llevar aparejada una ubicación distinta, naturalmente autónoma para el *cracking*" (Barrio Andrés, *Delitos 2.0. Aspectos penales, procesales y de seguridad de los ciberdelitos*, cit., pp. 107 y s). "De lo que se trata realmente es si debemos movernos para tutelar la integridad y disponibilidad de datos y sistemas en el ámbito de los delitos de daños o si, por el contrario, debemos prescindir de esta ubicación, atender la razón de ser de los preceptos que se han ido incorporado a la legislación penal en esta sede y proponer una absoluta tutela independiente que tenga en cuenta la posibilidad de atender directamente una nueva realidad criminal y un nuevo, por qué no, bien jurídico a tutelar vinculado a lo que hace surgir la normativa internacional: la preocupación por un mundo digital seguro que evite importantes perjuicios para el desarrollo, social y personal, de una ciudadanía que necesita de él" (De La Mata Barranco, Norberto. "La tutela de la integridad y disponibilidad de datos y sistemas informáticos: El modelo tradicional vinculado a una protección estrictamente patrimonial, un mal referente". En: Riquert, Marcelo A. [dir.] y Carlos Christian Sueiro [coord.]. *Sistema penal e informática. Ciberdelitos. Evidencia digital. TICS*, vol. 1. Buenos Aires: Hammurabi, 2019, p. 49).

> bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación, con la **finalidad de garantizar la lucha eficaz contra la ciberdelincuencia** [El resaltado es mío].

En los capítulos siguientes, analizaré los ciberdelitos dirigidos contra la seguridad informática, los cuales se encuentran regulados en los arts. 2, 3, 4, 7 y 10 de la LDI: Acceso ilícito, atentado contra datos y sistemas informáticos -conocidos genéricamente como *daños informáticos*[286]*-, interceptación ilícita y abuso de mecanismos y dispositivos informáticos.*

Para delimitar el marco conceptual que emplearé, en este capítulo abordaré las funciones preventiva y retributiva recogidas en la LDI, diferenciaré algunos términos como datos y sistemas informáticos -ya que serán empleados continuamente en los capítulossiguientes-, explicaré por qué es importante comprender que las TIC son el medio comisivo de estas modalidades delictivas, sostendré que el bien jurídico común de los cinco ilícitos analizados es la seguridad informática, describiendo sus tres componentes: confidencialidad, integridad y disponibilidad. Finalizaré el capítulo con algunas reflexiones en torno a dos elementos constitutivos de los tipos penales estudiados: la actuación deliberada e ilegítima.

4.2. FUNCIONES PREVENTIVAS Y RETRIBUTIVAS DE LA LDI

El artículo 1 LDI resalta la *función preventiva* de la legislación especial, debiéndose interpretar en concordancia con lo dispuesto en el artículo I del

286 Para comprender los alcances de este término, es importante analizar la legislación local estudiada por la doctrina consultada. Así, por ejemplo, en España se sostiene lo siguiente: "Bajo la expresión daños informáticos quedan aquí agrupadas un conjunto de conductas cuyo elemento común gira en torno a la integridad e indemnidad de los sistemas informáticos y de telecomunicaciones. Técnicamente, sólo los daños informáticos son considerados *stricto sensu* delitos contra el patrimonio, mientras que el sabotaje de telecomunicaciones aparece regulado por el Código Penal dentro de los delitos de desórdenes públicos por afectar a los sistemas generales de transmisión y comunicación. No obstante, el indudable parentesco entre las conductas de daños y el sabotaje informático aconsejan su estudio conjunto, sin perder de vista su distinta ubicación en el Código y el diferente bien jurídico afectado en uno y otro delito" (Flores Prada, Ignacio. *Criminalidad informática: aspectos sustantivos y procesales.* Valencia: Tirant lo Blanch, 2012, p. 168).

Título Preliminar del Código Penal: "Este Código tiene por objeto la prevención de delitos y faltas como medio protector de la persona humana y de la sociedad". Si bien la última norma utiliza la expresión *este código*[287], debe entenderse que la finalidad preventiva humanista irradia sus alcances a todo el ordenamiento punitivo, como es el especializado en ciberdelincuencia. De esta manera, si la legislación especial tuviese como objetivo únicamente la lucha eficaz contra la ciberdelincuencia, difícilmente superaría controles constitucionales, ya que sería un marco punitivo de orientación exclusivamente retributiva y no preventiva.

No debemos olvidar que el Derecho Penal es un *medio de control formal*, mientras que la familia, la escuela, la profesión y los grupos sociales poseen un *carácter informal*[288]. Así, como bien señala el profesor Castillo Alva, "la evitación y reducción de delitos no son tareas que solo le corresponden desarrollar al Estado, a través del Derecho Penal, sino a la comunidad en su conjunto [...]. Una adecuada estrategia preventiva es aquella que incide en políticas de índole

287 Castillo Alva, José Luis. "Finalidad del Código Penal". En: Salazar Sánchez, Nelson (dir.). *Comentarios al Código Penal peruano. Parte general*, Lima: Gaceta Jurídica, 2019, t. I, p. 20.

288 Mir Puig, Santiago. *Derecho penal. Parte general*. 6.ª edición (2.ª reimpresión). Barcelona: Reppertor, 2008, p. 47. "Hoy por hoy no se puede prescindir de la distinción entre orden social (control social informal) y orden jurídico (control social formal), cuyos titulares respectivos son la sociedad y el Estado, porque siempre tiene que existir una instancia superior y distinta que entre en funcionamiento cuando fracasen los mecanismos primarios de autoprotección del orden social y garantice eficazmente, en los conflictos más graves, la inviolabilidad de los valores fundamentales de la convivencia. Y ese es el cometido del orden jurídico" (García-Pablos De Molina, Antonio. *Derecho penal. Parte general: Fundamentos*. Lima: Jurista Editores, 2009, p. 130). En el mismo sentido: "[...] el Derecho Penal se caracteriza por prever las sanciones más graves -las penas y las medidas de seguridad-, como forma de evitar los comportamientos que juzgan especialmente peligrosos -los delitos-. En este sentido, el Derecho penal no puede arrogarse todo comportamiento social indeseado -su ámbito de aplicación es limitado-, sino solo aquellos que revisen suma gravedad y que no es posible de revertir con medios de control social menos severos. En esa línea de ideas, uno de los principales fundamentales legitimadores del Derecho penal es el principio de intervención mínima, admitidos unánimemente por la doctrina penal, según el cual el Derecho penal ha de reducir su intervención a aquello que sea estrictamente necesario en términos de utilidad social general [...]" (Ejecutoria Suprema del 12 de mayo de 1998. Recurso de Nulidad N.º 3763-2011-Huancavelica. Rojas Vargas, Fidel. *Código Penal. Parte general. Comentarios y jurisprudencia*. Lima: RZ, 2016, pp. 54 y 55).

social, económica o educativa con el fin de luchar contra el delito, dado que, si las causas del delito son estructurales o económicas, la mejor forma de contrarrestar a este es incidiendo en dichas causas o colocando obstáculos con tal fin. La mejor política criminal no es propiamente la que recurre al Derecho Penal, sino la que prescinde de él. Por tanto, una prevención adecuada y racional es la que privilegia otros controles o la política sociales antes que el Derecho penal"[289].

A nivel nacional, tres ejemplos de control social informal en materia de prevención de la ciberdelincuencia merecen ser destacados:

a. La Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros lidera una campaña llamada Alianza por una Internet Segura en el Perú[290] que reúne a Google, Microsoft, Cisco Networking Academy, Amazon Web Services, Meta, Save The Children, entre otras organizaciones y empresas para promover una cultura de prevención a favor de niños, niñas y adolescentes. Esta iniciativa reúne proyectos muy interesantes como Alto al ciberacoso[291], Conéctate sin riesgos[292], Navega tranqui[293] y Yo cuido mis datos personales[294].

b. La asociación Hiperderecho ha promovido diversos proyectos ciudadanos desde el 2012. El proyecto *10 derechos digitales que todo*

289 Castillo Alva, "Finalidad del Código Penal", cit., p. 21.

290 PCM. Alianza Nacional por una Internet Segura. Ver https://www.gob.pe/internetsegura

291 Este proyecto fue realizado por Movistar con el apoyo de Capital Humano y Social Alternativo, End Violence Against Children y Empresarios por la Educación. El objetivo: brindar un curso para prevenir, detectar y denunciar los riesgos del Internet.

292 Este proyecto fue organizado por el Ministerio de la Mujer y Poblaciones Vulnerables junto al Colectivo Child Rights Now, conformado por organizaciones internacionales como Aldeas SOS, Plan International, Save the Children, Terre des Hommes y World Vision. El objetivo: trabajar con padres, madres y docentes para generar acciones para la protección de los y las adolescentes en Internet.

293 Este proyecto fue organizado por Capital Humano Social Alternativo, junto a ECPAT y End Violence Against Children. El objetivo: prevenir la captación a través de redes sociales, en el delito de trata de seres humanos.

294 Este proyecto fue organizado por la Autoridad Nacional de Protección de Datos Personales del Ministerio de Justicia y Derechos Humanos. El objetivo: capacitar a niñas, niños y adolescentes en protección de su información en las redes sociales, para evitar que sean víctimas de ciberdelincuentes.

peruano debe defender[295] es uno de ellos y fue lanzado en el 2016 como "una forma de recordarnos la fragilidad de estos derechos y la necesidad de defender su ejercicio a diario en nuestro país". De manera muy ilustrativa, por ejemplo, explica que la privacidad se encuentra expuesta cuando "otros intentan vulnerar de forma ilícita nuestras contraseñas y otros mecanismos de seguridad para acceder a nuestra información personal". Como se puede apreciar, se resalta la función preventiva, desde la educación ciudadana, para evitar ser víctimas del delito de acceso ilícito.

En la misma línea, el proyecto *Tecnoresistencias*[296], publicado en el 2018, aborda diversos capítulos de la violencia de género en línea, con la finalidad de identificarla, reapropiarse de los espacios digitales perdidos o cedidos y denunciar la violencia en internet.



Imagen 8. El proyecto *Tecnoresistencias* constituye un espacio seguro para informarse adecuadamente y luchar contra la violencia de género en línea.

c. La Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC)[297] ha organizado diversos espacios colaborativos en los

295 Cfr. https://hiperderecho.org/10d/

296 Cfr. https://hiperderecho.org/tecnoresistencias/

297 Cuenta oficial de UNODC (Perú y Ecuador) en Twitter en la que se pueden encontrar otros proyectos: https://twitter.com/UNODC_PERU

que se promueve una cultura de prevención de la ciberdelincuencia. Así, por ejemplo, en el 2019, junto a la Municipalidad de Lima brindó talleres para combatir el *ciberbullying* y el ciberdelito en los colegios de Lima Cercado. En el 2021, deportistas de las selecciones de futsal y futbol playa de nuestro país participaron en un taller sobre prevención de amenazas en internet como parte del Programa Global de Ciberdelito e inciativa de The Education for Justice Initiative.

No se puede dejar de mencionar que el artículo 1 LDI también emplea la expresión *sancionar las conductas* como objetivo de la legislación, pues al lado de la prevención general y especial, la finalidad retributiva de la sanción siempre estará presente. Lo que sucede es que "hablar de Derecho penal es hablar, de un modo u otro, de violencia. Violentos son generalmente los casos de los que se ocupa el Derecho penal [...] Violenta es también la forma en que el Derecho penal soluciona estos casos (cárcel, internamientos psiquiátricos, suspensiones e inhabilitaciones de derechos)"[298]. Así, las sanciones previstas por el legislador alcanzan los 10 años de pena privativa de libertad en el caso de la interceptación de datos informáticos que comprometen la defensa, seguridad o soberanía nacional (art. 7 LDI) y en el fraude informático que afecta el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social (art. 8 LDI), sin contar las agravantes previstas en el artículo 11 LDI. Es más, el legislador peruano, a fines del 2024, introdujo el delito de préstamo informático extorsivo (art. 8-A LDI) que sanciona hasta con 15 años de pena privativa de libertad, en su modalidad básica. Como vemos, si bien nuestra legislación especial se orienta a la prevención, también reconoce el castigo como uno de sus objetivos.

4.3. SISTEMAS Y DATOS INFORMÁTICOS

El miércoles 21 de junio de 2000, en el Congreso se discutió la incorporación de los primeros delitos informáticos al Código Penal. Una de las observaciones formuladas por el Poder Ejecutivo giraba en torno al uso de expresiones como base de datos o redes informáticas en la propuesta normativa inicial. En este sentido, si bien se recomendó emplear la expresión *sistemas informáticos*,

298 Muñoz Conde, Francisco y Mercedes García Arán. *Derecho penal. Parte general.* 7.ª edición, revisada y puesta al día. Valencia: Tirant lo Blanch, 2007, p. 29.

nuestros legisladores la rechazaron argumentando que nos encontrábamos frente a un término vago e impreciso:

> La tercera observación del Ejecutivo es la denominación de base de datos, las redes, elementos informáticos integrantes del computador, que debería resumirse en la denominación "sistema informático".
>
> Respuesta: No es posible darle un contenido gramatical general, como decir "sistema informático", a situaciones o bienes que conjugan o integran este sistema, porque base de datos, redes, elementos informáticos, son utilizados de manera muy general por distintas entidades y personas. Por lo tanto, cuando se observa esta ley señalando que mejor utilicemos la denominación general "sistema informático", digo que esta definición es imprecisa dentro de nuestra legislación nacional y, sobre todo, de la legislación internacional.
>
> En consecuencia, tanto en la doctrina como en la legislación comparada no encontramos ninguna definición que diga, efectivamente, que "sistema informático" engloba a todo lo que es base de datos, redes o elementos informáticos. En tal sentido, el Congreso debe insistir en esta postura[299].

Como se señaló en el segundo capítulo, en el 2001, el Convenio de Budapest se erigiría como el principal instrumento de lucha contra este fenómeno delictivo, recogiendo como parte de la terminología recomendada a los Estados dos conceptos: datos y sistemas informáticos. De este modo, poco más de dos décadas después de la discusión legislativa analizada, se puede afirmar que el Ejecutivo tenía la razón: el empleo de *sistemas informáticos* hubiese permitido, desde el inicio, comprender uno de los objetos de protección de legislación especializada en cibercriminalidad.

En las líneas siguientes analizaremos precisamente estos dos conceptos, pues serán empleados de forma reiterada en diversos tipos penales previstos en la LDI.

299 Novena sesión vespertina del miércoles 21 de junio del 2000, bajo la presidencia de la señora Martha Hildebrandt Pérez-Treviño. p. 921.

4.3.1. Sistemas informáticos

La expresión *sistema informático* es utilizada en ocho artículos de la LDI[300], razón por la que establecer una definición clara es una labor importante, pero nada sencilla. Así, por ejemplo, la Convención de la Unión Africana sobre Ciberseguridad y Protección de Datos Personales, adoptada en el 2014, lo define como:

> **Art. 1.- Definitions**
>
> [...]
>
> **Computer system** means an electronic, magnetic, optical, electrochemical, or other high speed data processing device or a group of interconnected or related devices performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or devices; [**Sistema Informático.** Todo dispositivo electrónico, magnético, óptico o electroquímico de procesamiento de datos a alta velocidad o conjunto de dispositivos interconectados o relacionados que realiza funciones de lógica, aritmética o almacenamiento, incluyendo medios de almacenamiento de datos o medios de comunicación directamente relacionados o que operan en conjunto con ese dispositivo o dispositivos (traducción libre)]

De otro lado, la Convención Árabe Relativa a la Lucha contra los Delitos de la Tecnología de la Información, adoptada por la Liga de los Estados Árabes, en el 2010, emplea la siguiente acepción:

> **Art. 2.-**
>
> [...]
>
> **5. Information system:** A set of programmes and tools intended to process and manage data and information [**5. Sistema Informático.**

300 **LDI, art.1** (objeto de la ley), **art. 2** (acceso ilícito), **art. 4** (atentado a la integridad de sistemas informáticos), **art. 7** (interceptación de datos informáticos), **art. 8** (fraude informático), **art. 12** (exención de responsabilidad penal), **sexta disposición complementaria final** (medidas de seguridad) y **novena disposición complementaria final** (terminología).

> Un conjunto de programas y herramientas destinado a procesar y gestionar datos e información (traducción libre)]

En el ámbito local, Perú recoge la definición desarrollada en el Convenio sobre la Ciberdelincuencia. De este modo, en la novena disposición complementaria final de la LDI, se define el sistema informático:

> **NOVENA. Terminología.** Para efectos de la presente ley, se entenderá, de conformidad con el artículo 1 del Convenio sobre la Ciberdelincuencia, 23.XI.2001:
>
> a. **Por sistema informático:** todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa.

El Informe Explicativo del Convenio sobre la Ciberdelincuencia precisa que un sistema informático "es un dispositivo que consta de *hardware* y *software*, cuya función es el tratamiento automatizado de datos digitales. Puede incluir facilidades de entrada (*input*), salida (*output*) y almacenamiento. Puede funcionar en forma independiente o estar conectado a una red de dispositivos similares"[301].

Dicho esto, un sistema informático puede ser una computadora, una laptop, una tableta, un celular o, simplemente, los dispositivos de Internet de las cosas (IoT) -entre ellos, relojes y electrodomésticos inteligentes-. Está formado por un componente físico (*hardware*) y uno lógico (*software*). Entre los primeros recursos se encuentran los servidores y estaciones de trabajo, ordenadores portátiles, impresoras, escáneres y otros periféricos. En los segundos: los sistemas operativos, herramientas ofimáticas, software de gestión, herramientas de programación, aplicaciones desarrolladas a medidas, entre otros[302].

En el Informe Explicativo[303] antes mencionado se desarrollan dos términos adicionales que están vinculados al funcionamiento de los sistemas en

301 Fundamento 23 del Informe Explicativo.

302 Gómez Vieites, Álvaro. *Enciclopedia de la Seguridad Informática*. Madrid: RA-MA Editorial y Publicaciones. [Kindle]

303 Fundamento 23 del Informe Explicativo.

referencia: *automatizado* y *tratamiento de datos*. El primero significa 'sin intervención directa de un ser humano', mientras que el segundo explica que 'los datos que se encuentran en un sistema informático son operados mediante la ejecución de un programa informático'.

Por otro lado, un *programa informático* es un "conjunto de instrucciones que pueden ser ejecutadas por el equipo para alcanzar el resultado deseado. Un equipo puede ejecutar diversos programas"[304].

Finalmente, una *red* es una "interconexión entre dos o más sistemas informáticos. Las conexiones pueden ser terrestres (por ej., alámbricas o por cable), inalámbricas (por ej., radioeléctricas, infrarrojas o satelitales), o de ambos tipos. Una red puede estar limitada geográficamente a un área pequeña (redes de área local) o puede abarcar un área extensa (redes de área extensa), y esas redes pueden a su vez estar interconectadas"[305].

Antes de finalizar este apartado, es importante señalar que la Convención de las Naciones Unidas contra la Ciberdelincuencia no recoge la expresión *sistema informático*, sino *sistema de tecnología de la información y las comunicaciones*, definiéndolo en los siguientes términos:

> Todo dispositivo o conjunto de dispositivos interconectados o relacionados entre sí cuya función, o la de alguno de sus elementos, sea reunir, almacenar y procesar automáticamente datos electrónicos mediante la ejecución de un programa.

4.3.2. Datos informáticos

Este elemento es empleado también en ocho artículos de la Ley de Delitos Informáticos[306]. Al igual que en el caso anterior, nos encon-

304 Fundamento 23 del Informe Explicativo.

305 Fundamento 24 del Informe Explicativo.

306 **Ley de Delitos Informáticos, art.1** (objeto de la ley), **art. 3** (atentado a la integridad de datos informáticos), **art. 7** (interceptación de datos informáticos), **art. 8** (fraude informático), **art. 10** (abuso de mecanismos y dispositivos informáticos), primera disposición complementaria final (codificación de la pornografía infantil), sexta disposición complementaria final (medidas de seguridad) y novena disposición complementaria final (terminología).

tramos ante una expresión polisémica, ya que puede recibir diversos significados. Por esta razón, el lector, en primer lugar, debe diferenciar *dato* de *dato informático*. El primero puede referirse a información educativa, de salud, de trabajo, entre otros -que no se encuentra necesariamente en línea-. El segundo se refiere a representaciones que se prestan al procesamiento automatizado, en formatos electrónicos u otro que pueda ser procesado por un sistema informático[307].

Retomando los dos instrumentos internacionales antes empleados, la Convención de la Unión Africana sobre Ciberseguridad y Protección de Datos Personales define los *datos informáticos o computarizados* de la siguiente forma:

> **Art. 1.- Dato computarizado** significa cualquier representación de hechos, información o conceptos en una forma adecuada para su procesamiento en un sistema informático. [Traducción libre][308]

En la misma línea, la Convención Árabe Relativa a la Lucha contra los Delitos de la Tecnología de la Información también define datos informáticos empleando una fórmula similar:

> **Art. 2.- 3. Dato informático.** Todo lo que se puede almacenar, procesar, generar y transferir mediante la tecnología de la información, como números, letras, símbolos, etc. [Traducción libre][309]

La Ley de Delitos Informáticos recoge la definición prevista en el Convenio de Budapest en los siguientes términos:

> **NOVENA. Terminología.** Para efectos de la presente ley, se entenderá, de conformidad con el artículo 1 del Convenio sobre la Ciberdelincuencia, 23.XI.2001:

307 Sobre este punto, el Informe Explicativo precisa que "con el fin de aclarar que en el presente Convenio el término *datos* debe entenderse como datos en formato electrónico u otro formato que se preste a tratamiento informático directamente, se introduce el concepto de *datos informáticos*" (fundamento 25 del Informe Explicativo).

308 **Computerized data** means any representation of facts, information or concepts in a form suitable for processing in a computer system.

309 **Data:** All that may be stored, processed, generated and transferred by means of information technology, such as numbers, letters, symbols, etc.

b. **Por dato informático:** toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función.

El Informe Explicativo del Convenio sobre la Cibercriminalidad precisa que la definición toma como base la ISO y que la expresión *que se preste a tratamiento informático* significa que 'los datos están en un formato tal que pueden ser procesados directamente por un sistema informático'.

Los datos informáticos que se procesan automáticamente, precisa el Informe Explicativo, "pueden ser objeto de uno de los delitos definidos en el presente Convenio, así como el objeto de la solicitud de una de las medidas de investigación definidas en el presente Convenio". Dicho de otro modo, los datos informáticos pueden ser tanto objeto del delito como objeto de investigación.

Dicho esto, siguiendo los instrumentos antes mencionados, el dato informático será toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función.

Ahora bien, la Convención de las Naciones Unidas contra la Ciberdelincuencia no utiliza la expresión dato informático, sino *dato electrónico*, definiéndolo como "toda representación de hechos, información o conceptos de una forma apta para el procesamiento mediante un sistema de tecnología de información y las comunicaciones, incluido un programa adecuado para que un sistema de tecnología de la información y las comunicaciones ejecute una función". Como se puede apreciar, ambas definiciones son muy similares.

No debemos olvidar que el dato informático puede ser tanto objeto de delito -por ejemplo, en los daños informáticos-, como objeto de una medida de investigación -cuando el Ministerio Público requiere datos de suscriptor, tráfico o contenido en una investigación criminal[310]-.

310 Marcelo Temperini explica la diferencia de estos tres conceptos y la intensidad de la afectación que puede generar una investigación criminal sobre los derechos constitucionales del indagado. Así, utiliza la expresión *la regla de los tres escalones* para graficarlo. Los datos del suscriptor o del abonado están en el primer escalón e incluyen: nombre de la cuenta, nombre de usuario o de acceso, nombre y apellidos registrados, domicilios registrados, correo electrónico registrado, número de teléfonos asociados a

En el centro de la sociedad y de la economía, actualmente se encuentran los datos informáticos. Su generación, almacenamiento, seguridad y explotación son muy importantes para la investigación e innovación tecnológica, ya que impulsan la transformación digital, permiten mejorar la eficiencia de las empresas y su adecuado tratamiento puede impactar en productos y servicios que mejoren la calidad de vida de la población[311].

4.4. EL USO DE LAS TIC COMO MEDIO COMISIVO

Al promulgarse la LDI, los artículos 3, 4, 5, 7 y 9 incluían la expresión *mediante las tecnologías de la información o de la comunicación* como medio para la comisión del acto ilícito; sin embargo, la Ley N.º 30171 de marzo del 2014 la eliminó de los artículos 3, 4, 5 y 7, dejándola únicamente en el delito de suplantación de identidad. El 13 diciembre del 2023, mediante Decreto Legislativo N.º 1591 se modificó este delito, variando el elemento bajo estudio por el de *tecnologías digitales*.

Para comprender la modificación inicial, nos debemos remontar a fines del 2013, cuando los congresistas Juan Carlos Eguren y Mauricio Mulder presentaron dos proyectos de ley[312] orientados, entre otras razones, a eliminar

---

la cuenta, dirección IP utilizada al momento de la creación de la cuenta, fecha y hora de creación de la cuenta, información de sesiones iniciadas, entre otros. En el segundo escalón se encuentran los datos de tráfico, datos asociados, datos transaccionales o metadatos de la comunicación. En esta categoría se encuentran los registros de un servidor que guarda las comunicaciones electrónicas entrantes y salientes, IP de origen y destino de la comunicación, fecha, hora y ruta de la comunicación. Finalmente, en el último peldaño se ubican los datos de contenido y constituye el mensaje en sí mismo (Temperini, Marcelo. "Delitos informáticos y cibercrimen: Técnicas y tendencias de investigación penal y su afectación a los derechos constitucionales". En: Dupuy, Daniela [dir.]. *Cibercrimen II. Nuevas conductas penales y contravencionales. Inteligencia artificial aplicada al derecho penal y procesal penal. Novedosos medios probatorios para recolectar evidencia digital. Cooperación internacional y victimología*. Montevideo: B de F, 2018, pp. 224-241).

311 Martínez Alba, Flores. "La transformación digital del dato: nuevos usos y nuevos métodos". En: Perea Ortega, Rafael (dir.). *Estudios sobre derecho digital*. Navarra: Thomson Reuters / Aranzadi, 2021.

312 Congreso de la República del Perú. *Proyecto de Ley N.º 2991/2013-CR, proyecto de ley que modifica la ley 30096, Ley de Delitos Informáticos*. Presentado el 25 de noviembre del 2013.

la expresión *tecnologías de la información o comunicación* de la configuración de los tipos penales antes mencionados. Si bien en la exposición de motivos de ambos proyectos de ley no se exteriorizan las razones, infiero que lo hicieron por la preocupación expuesta por diferentes sectores de la comunidad académica e informática y para que la LDI contara con una redacción mucho más cercana a lo establecido en el Convenio de Budapest. Esta conjetura la sostengo en base a lo expuesto en el debate suscitado el 12 de febrero de 2014, fecha en la que se plantearon las modificaciones propuestas a la LDI:

> El señor Eguren Neuenschwander (PPC-APP).- [...] Como los señores parlamentarios recordarán, que dio una ley, la 30096, Ley de Delitos Informáticos. Una iniciativa que se convirtió en ley importante, porque nos pone en un escenario de modernidad en la lucha contra la ciberdelincuencia en la serie de modalidades que permanentemente están en proceso de avance, en la medida y en paralelo al avance tecnológico.
>
> Sin embargo, **esta ley generó preocupación en muchos de los destinatarios de la norma**, fundamentalmente la gente vinculada a las tecnologías de la información y comunicación que no necesariamente son abogados.
>
> En consecuencia, hubo varios artículos que generaron suspicacia, generaron preocupaciones que dio lugar a que se presenten tres proyectos de ley. Los mismos que han sido recogidos mayoritariamente en este dictamen, donde se hace una serie de precisiones para evitar preocupaciones, dudas, suspicacias. Básicamente porque al ser una ley especial de carácter penal, tiene que estar referida en el marco del Código Penal, y específicamente a la parte de régimen general donde se habla de dolo, daño, una actitud deliberada, ilegítimamente, temas que no estaban expresamente señalados en la Ley de Delitos Informáticos, porque se entienden que, al ser una norma penal, está dentro del marco de régimen general.
>
> Sin embargo, repito, estas preocupaciones creo válidas, creo legítimas, han sido recogidas en el proyecto de ley [...]
>
> La señora Solórzano Flores (NGP).- [...] Solamente para disipar dudas, me gustaría que el presidente de la comisión también haga referencia un poquito más específicamente a lo que es [el] Convenio de Budapest. Si bien es cierto, hay otros países que no son parte de este

> Convenio, cuál sería el efecto vinculante al pretender el día de hoy nosotros, bueno, ya lo hemos tipificado, ya tenemos incluso esta Ley de Delitos Informáticos.
>
> El día de hoy estamos modificando algunos aspectos que se discutió bastante en los medios y creo que es saludable estas modificaciones, pero si para que el presidente de la Comisión diga cuál es el post respecto a la injerencia a que el Perú pertenezca o firme este Convenio de Budapest, en todo caso cuál sería si hay algún tipo de contra versión con lo que estamos tipificando el día de hoy [...]
>
> El señor EGUREN NEUENSCHWANDER (PPC-APP).- [...] Le agradezco a la congresista Solórzano. El Perú no es parte del Convenio de Budapest, pero sí es un convenio que es para aquellos incluso que no somos parte ni estamos obligados, es un convenio que orienta a todos los países en el desarrollo de su legislación.
>
> Y entre la ley aprobada y estas mejores incorporaciones, estamos pretendiendo alinearnos mucho más al Convenio de Budapest que, es un referente internacional, que seguramente la mayor parte de países del mundo están pretendiendo ese lineamiento, porque este tipo de delitos, por las características del instrumento, -que en muchos casos es la internet- no tiene un límite geográfico, no son presenciales, son a distancia [...]
>
> En consecuencia, es importante que los países, en la medida de lo posible, homologuen su tratamiento penal para poder tener niveles de colaboración mutua. Entonces, **en la medida que las legislaciones sean lo más parecidas posibles vamos a poder tener en este mundo globalizado e interconectado, mejor capacidad para luchar contra la delincuencia** [El resaltado es mío][313].

En efecto, los delitos recogidos en el Convenio de Budapest no precisan que su comisión se realice mediante el uso de las TIC; sin embargo, el Informe Explicativo del citado convenio aclara que sí es necesario, pero dependerá de cada Estado identificar la mejor técnica legislativa para dichos fines:

313 Octava sesión matinal del 12 de febrero de 2014, bajo la presidencia de los señores Fredy Otárola Peñaranda, Carmen Omonte Durand y José León Luna Gálvez. pp. 57, 60 y 61.

> 36. Si bien **las disposiciones del derecho sustantivo se refieren a delitos que utilizan la tecnología de la información**, el Convenio utiliza un lenguaje neutro en cuanto a la tecnología de manera tal que los delitos contemplados en el derecho penal puedan aplicarse tanto a las tecnologías actuales como a las futuras [El resaltado es mío].
>
> 41. Las leyes que establecen estos delitos deberían ser redactadas con la mayor claridad y especificidad posible, con el fin de prever adecuadamente los tipos de conducta pasibles de una sanción penal.

En el escenario peruano actual, ¿los delitos de atentados contra la integridad de los datos informáticos, sistemas informáticos, *child grooming* e interceptación de datos informáticos -previstos en la LDI- exigen el uso de las TIC para su comisión? Dicho de otra forma, ¿se requiere o no el empleo de las TIC para la realización de los delitos informáticos? Sostengo que sí, pues el artículo 1 es una norma que orienta la interpretación y los alcances de la LDI. En consecuencia, a pesar de la modificación, los delitos previstos en los capítulos II al VI de la LDI sí exigen que la conducta se desplegué mediante el empleo de las TIC o, a la luz del Informe Explicativo, a través de las tecnologías.

Si no interpretamos los tipos penales de la LDI bajo los alcances del artículo 1, podríamos llegar a los siguientes escenarios absurdos:

1. Prender fuego a un USB que contiene archivos sería atentar contra la integridad de los datos informáticos.
2. Destruir físicamente una computadora conectada a una red sería atentar contra la integridad de los sistemas informáticos.
3. Romper la chapa de la puerta para ingresar a una oficina y ver la computadora que su propietario dejó encendida al salir, configuraría acceso ilícito, en la modalidad de vulneración de las medidas de seguridad.

En este sentido, considero que el empleo de las TIC[314] -o, mínimamente, de la tecnología- es el medio para la comisión de los delitos previstos en la LDI.

---

314 Autores como Juan Carlos Díaz Colchado y Andreé Castro Arequipeño, siguiendo a Díaz Revorio y Raúl Oroño, prefieren utilizar la expresión *Nuevas TIC's* para destacar que la tecnología evoluciona y se renueva constantemente. Así, señalan que el

4.5. BIENES JURÍDICOS PROTEGIDOS EN LA LDI

Sobre este tópico, la profesora chilena Laura Mayer sostiene que, a nivel doctrinario, es posible diferenciar dos teorías vinculadas con la forma que adopta la tipificación de los delitos informáticos, según el bien jurídico protegido[315]:

a) La primera tesis asume que los delitos informáticos tutelan un bien jurídico específico, propiamente informático, diverso del que protegen los delitos tradicionales. La autora ejemplifica esta posición con la Ley chilena N.º 19223, publicada el 7 de junio de 1993, que, en vez de modificar el marco normativo existente, prefirió regular el fenómeno fuera del Código Penal.

b) La segunda tesis considera que la diferencia es de forma y no de fondo, pues los delitos informáticos solo actualizan el modo cómo se delinque, ya que los delitos siguen siendo tradicionales y los bienes jurídicos también. Así, se continúa protegiendo el patrimonio, la intimidad, la fe pública, pero, se criminalizan nuevas formas de comisión.

El 13 de noviembre del 2014, la congresista Martha Chávez Cossio presentó el proyecto de Ley N.º 3980/2014 con el objeto de modificar el artículo 1 de la LDI. Según la legisladora, la redacción recogida era errónea, "pues los bienes jurídicos protegidos no son los sistemas y datos informáticos, sino la propiedad, la protección de datos personales y la intimidad de las personas contenidos en ellos [...]. Precisamente, el art. I del Título Preliminar del Código Penal señala que tiene por objeto la prevención de delitos como medio protector

último autor explica que "la característica de 'nueva' se refiere a que antes ya existían tecnologías, las cuales se van renovando constantemente. Es por ello que cobra sentido el ser nuevas, puesto que siempre existirá una más moderna que otra, en tanto que por tecnología entiende el uso de materiales, instrumentos, técnicas y fuentes de energía a fin de facilitar la vida y hacer más productivo el desarrollo del trabajo" (Díaz Colchado/Castro Arequipeño, "Los derechos fundamentales y las nuevas tecnologías de la información y comunicación: Una aproximación", cit., pp. 16 y s).

315 Mayer Lux, Laura. "El bien jurídico protegido en los delitos informáticos". En: *Revista Chilena de Derecho*. Vol. 44. N.º 1. Santiago: 2017, pp. 238 y s. https://www.scielo.cl/pdf/rchilder/v44n1/art11.pdf

de la persona y de la sociedad"[316]. A partir de esta propuesta, merece la pena responder la siguiente pregunta: ¿la LDI protege algún bien jurídico común a cada ilícito previsto en la norma? Considero que no. Cada delito que integra la LDI protege uno o más bienes jurídicos penalmente relevantes.

En efecto, hace casi treinta años, en 1997, el profesor Bramont-Arias Torres sostenía que los delitos informáticos no tutelan un único bien jurídico protegido -posición que comparto-, sino que, dependiendo del tipo de ataque, se pueden afectar uno o más:

> Es innegable el hecho de que los diferentes comportamientos incluidos dentro del delito informático pueden afectar múltiples bienes jurídicos; de hecho, ha quedado demostrado como la intimidad, el patrimonio, el orden económico resultan lesionados mediante manipulación informática de datos. Pero no solo ellos, también es posible hablar de la seguridad nacional, la seguridad del flujo transnacional de datos, etc.
>
> De manera indiscriminada, pues, se alude a bienes jurídicos de naturaleza individual como macrosocial. Todo ello nos obliga a afirmar que en realidad no existe un bien jurídico protegido en el delito informático, porque en verdad no hay, como tal un "delito" informático. Este no es más que una forma o método de ejecución de conductas delictivas que afectan a bienes jurídicos que ya gozan de una específica protección por el Derecho Penal.
>
> Así, sería más correcto hablar de criminalidad informática en cuanto nueva forma de comisión de delitos ya tradicionales, como puede ser la estafa, el hurto, el delito de traición a la patria, espionaje, nacida al amparo del rápido desarrollo tecnológico habido en los últimos tiempos[317].

316 La congresista propuso modificar el art. 1 en los siguientes términos: "La presente Ley tiene por objeto prevenir y sancionar las conductas ilícitas que afectan el derecho a la propiedad, la protección de los datos personales y la intimidad de las personas contenidos en los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia".

317 Bramont-Arias Torres, *El delito informático en el Código Penal peruano*, cit., p. 58.

En efecto, esta fue la posición que tomó nuestro legislador al promulgar la Ley de Delitos Informáticos: se estableció un cuerpo normativo de delitos que compartían características similares, pero divididos según el objeto de protección. De este modo, a la fecha, tenemos la siguiente distribución:

a) Delitos informáticos contra datos y sistemas informáticos: acceso ilícito (art. 2 LDI), atentado a la integridad de datos informáticos (art. 3 LDI), atentado contra la integridad de sistemas informáticos (art. 4 LDI).

b) Delitos informáticos contra la indemnidad y libertad sexuales: proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos (art. 5 LDI), chantaje sexual con materiales elaborados o modificados por medios digitales o tecnológicos (art. 5-A LDI).

c) Delitos informáticos contra la intimidad y el secreto de las comunicaciones: interceptación de datos informáticos (art. 7 LDI).

d) Delitos informáticos contra el patrimonio: fraude informático (art. 8 LDI), préstamos informáticos extorsivos (art. 8-A LDI).

e) Delitos informáticos contra la fe pública: suplantación de identidad (art. 9 LDI).

Como se puede apreciar, cada capítulo puede asociarse con un bien jurídico protegido, sin embargo, advierto algunos problemas.

Primero, los datos y los sistemas informáticos no son bienes jurídicos, mientras que su relación con el usuario, sí. De este modo, como desarrollaré más adelante, lo que el ordenamiento debe tutelar es la confidencialidad, la integridad y la disponibilidad de aquellos datos y sistemas; es decir, la seguridad informática[318].

Segundo, el legislador confunde la intimidad, el secreto de las comunicaciones y la confidencialidad. Al referirnos a los datos o los sistemas informáticos, no se busca proteger la *intimidad* del usuario o su *secreto de las comunicaciones*,

318 "[Si] se afirma que los delitos informáticos protegen la información contenida en un sistema informático ¿por qué no podría sostenerse que la falsedad documental protege la información plasmada en un soporte documental? En cambio, la doctrina ha optado por formular el objeto de tutela de las falsedades documentales en otros términos, teniendo en cuenta las funciones que esos soportes desempeñan en el tráfico jurídico y no la información en sí misma" (Mayer Lux, "El bien jurídico protegido en los delitos informáticos", cit., p. 241).

sino su confidencialidad. Este concepto será desarrollado más adelante. En este punto, basta con señalar que son conceptos distintos.

Tercero, el legislador tipificó también el delito de abuso de mecanismos y dispositivos informáticos (art. 10 LDI), sin embargo, lo incluyó en el capítulo denominado "Disposiciones comunes". Considero que debió incluirlo en uno titulado *Delitos contra la seguridad informática* -agrupación que es propuesta, a su vez, por el Convenio de Budapest y la Convención de las Naciones Unidas contra la Ciberdelincuencia-.

4.6. LA SEGURIDAD INFORMÁTICA COMO BIEN JURÍDICO PROTEGIDO

4.6.1. Definición de *seguridad informática*

La seguridad informática es definida como "cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema"[319]. Es importante indicar que, en algunos casos, las expresiones *seguridad de la información* y *ciberseguridad*[320] son utilizadas como sinónimos.

En la norma ISO/IEC 17799, Tecnología de la información-Técnicas de seguridad-Código para la práctica de la seguridad de la información, la seguridad informática se define como la "preservación de confidencialidad, integración y disponibilidad de la información; además, también puede involucrar otras propiedades como autenticidad, responsabilidad, no repudiación y confidencialidad".

---

319 Gómez Vieites, Álvaro. *Enciclopedia de la Seguridad Informática*. Madrid: RA-MA Editorial y Publicaciones. [Kindle]

320 "La ciberseguridad es la seguridad informática: La práctica de proteger los ordenadores y sus datos de la amenaza. Los hackers son muy útiles en ciberseguridad, porque encuentran usos novedosos de la tecnología" (Crawley, Kim. *Cultura hacker de la A a la Z. Una guía divertida de las personas, ideas y artefactos que han construido el mundo de la tecnología*. Madrid: Ediciones Anaya Multimedia, 2024, p. 58). En la misma línea: "Cibersecurity: Protection against unauthorized use of computers, computer systems, and / or electronic data" (Kremling, Janine y Amanda M. Sharp Parker. *Cyberspace, Cybersecurity, and Cybercrime*. Thousand Oaks: Sage Publications, 2017, p. 226).

De acuerdo al National Institute of Standars and Technology del U. S. Deparment of Commerce, la seguridad informática es

> The protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats. [La protección de los sistemas de información contra el acceso no autorizado o la modificación de la información, ya sea durante su almacenamiento, procesamiento o transmisión, así como contra la denegación de servicio a usuarios autorizados, incluyendo las medidas necesarias para detectar, documentar y contrarrestar dichas amenazas][321]. [Traducción propia].

En esta línea, en la sección Términos y definiciones de la Política Nacional de Ciberseguridad peruana, se define la seguridad informática como:

> La preservación de las siguientes características: Confidencialidad (Garantizar que la información sea accesible solo a aquellas personas autorizadas a tener acceso a la misma), Integridad (Salvaguardar la exactitud y totalidad de la información y los métodos de procesamiento) y Disponibilidad (Garantizar que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran)[322].

A nivel jurisprudencial, el concepto *seguridad informática* ha sido mencionado por la Corte Suprema en una ocasión. Así, en el Recurso de Casación N.º 453-2022/Nacional, del 4 de noviembre de 2024, se señala lo siguiente:

> Es evidente, como una máxima de la experiencia, que todo sistema informático, más aún si tiene un determinado tiempo de aplicación,

321 Cfr. "Information systems security (INFOSEC)". https://csrc.nist.gov/glossary/term/information_systems_security

322 Cfr. *Política Nacional de Ciberseguridad.* PCM. Secretaría de Gobierno Digital [Lima: 2017]. https://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/A36311FB344A1DC7052583160057706D/$FILE/Política_Nacional_de_Ciberseguridad_peru.pdf

> puede ser vulnerado, de ahí que una regla es que periódicamente se refuerce y se introduzcan nuevas pautas técnicas y de **seguridad informática** [El resaltado es mío].

Nuestras vidas han incorporado el uso de las TIC en el día a día y en todo ámbito: personal, laboral, académico, de salud, finanzas, etcétera. Dicho esto, los bienes jurídicos tradicionales no son los únicos que pueden ser lesionados cuando se vulnera el uso correcto de datos y sistemas informáticos; de ahí que la legislación comparada y los esfuerzos internacionales apunten a la protección de un nuevo bien jurídico protegido: la seguridad informática[323].

4.6.2. La seguridad informática como bien jurídico protegido

Llegado a este punto, debo indicar que sobre la protección de un bien jurídico en determinados tipos de delitos -en particular, los estudiados en esta

323 Sobre este punto, las reflexiones del profesor De La Mata Barranco son muy claras: "¿Cómo hacer frente a esas conductas? ¿Adaptando -o ampliando- los tipos penales existentes y relacionando estas conductas con bienes jurídicos objeto de tradicional tutela penal, como en Europa? [...]. Lo que está claro es que frente al avance de las nuevas tecnologías, el Derecho penal sustantivo más reciente se ha revelado insuficiente, pues la protección del domicilio, de la correspondencia, del secreto profesional, de la imagen, de las palabras se enfrenta, como antes se decía, con una realidad 'virtual' que la sobrepasa en un mundo en que todo se digitaliza, en que 'somos en datos' y que quien conoce los algoritmos se informa de lo que somos y toma decisiones sobre lo que somos que puede impedir que seamos lo que queremos ser. [...] No obstante, en el año 2000 se dicta la Resolución de la Asamblea General de Naciones Unidas a/res/55/63, de 22 de enero, en la que se alude a la necesidad de crear un marco normativo que proteja la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos y se penalice su uso y deterioro no autorizado, sin exigir que se produzca un daño a bienes jurídicos tradicionales, pero enfatizando la también necesidad de proteger tanto la libertad individual como la privacidad. **La cuestión, tal y como se va planteando es la de o bien atender directamente la tutela de la "seguridad" informática (con esta u otra denominación), la tutela de datos y sistemas,** adelantando la intervención penal o, por el contrario, seguir exigiendo que se afecten intereses individuales. Ambas propuestas pueden ser compatibles, distinguiendo, como se ha reiterado, los delitos informáticos en su sentido más estricto (o contra las nuevas o altas tecnologías) de los delitos contenidos" [el resaltado es mío] (De La Mata Barranco, Norberto. "Reflexiones sobre el bien jurídico a proteger en el delito de acceso ilícito [art. 197 bis CP]. El concepto de privacidad informática y la tutela del buen funcionamiento de los sistemas de información y comunicación". En: *Cuadernos de Política Criminal* 118. Madrid: 2016, pp. 78 y s).

obra-, se identifican principalmente dos posiciones[324]. Así, hay quienes consideran lo siguiente:

a) Se protege la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos. Siguiendo la fórmula propuesta en el Convenio de Budapest, se sostiene que estos elementos son objeto de protección exclusivo en determinados tipos penales. Sin embargo, se critica que no puede existir una protección copulativa, ya que habrá algunos delitos que lesionen la confidencialidad, pero no la integridad ni la disponibilidad. De otro lado, también se sostiene que estos atributos no son más que una reformulación de bienes jurídicos clásicos. Así, la confidencialidad sería una extensión o nueva interpretación de la intimidad o privacidad, mientras que la integridad y disponibilidad se asimilan a las características propias de la propiedad[325].

b) Se protege el correcto funcionamiento del procesamiento de datos. De acuerdo con la profesora Mayer, "la doctrina alemana constituye un claro ejemplo de reconocimiento marginal de bienes jurídicos específicos, propiamente informáticos. Según ella, la consagración de delitos informáticos ha buscado extender los tipos penales clásicos, a fin de colmar los vacíos que pudiera generar el componente informático en la comisión de ciertas conductas. Por

---

324 Con algunos matices, algunos autores han propuesto que el objeto de protección es la información. En el 2006, por ejemplo, se sostenía lo siguiente: "Como se desarrollará en el presente trabajo, consideramos que la primera opción es la correcta; es decir, el avance tecnológico que representa Internet y los problemas presentados por el uso generalizado de los sistemas informáticos disparan necesidades propias para el derecho penal, que ahora tiene ante sí un nuevo interés social digno de protección: la información y su transmisión a través de los sistemas telemáticos [...]. La protección de la información (almacenada, tratada y transmitida mediante los sistemas de procesamiento de datos) como valor económico de la empresa, que confiere a su titular una posición ventajosa en las relaciones de tráfico económico, es un interés social digno de tutela penal, que, frente a una forma de criminalidad considerada, no sin razón, como el 'delito de futuro', tendría que justificar, sin lugar a dudas, estos esfuerzos" (Aboso, Gustavo Eduardo y María Florencia Zapata. *Cibercriminalidad y derecho penal. La información y los sistemas informáticos como nuevo paradigma del derecho penal. Análisis doctrinario, jurisprudencial y derecho comparado sobre los denominados delitos informáticos*. Montevideo: B de F, 2006, pp. 15, 16 y 18).

325 Mayer Lux, "El bien jurídico protegido en los delitos informáticos", cit., pp. 245 y s.

lo mismo, salvo contadas excepciones, los intereses subyacentes a tales ilícitos son abordados fundamentalmente como reformulaciones de bienes jurídicos tradicionales"[326].

Tal y como adelanté, considero que la seguridad informática[327] se erige como el *bien jurídico protegido y constitucionalmente relevante,* reconocimiento que ayudará a interpretar los alcances de los delitos analizados en esta obra: acceso ilícito, atentado contra datos informáticos y contra sistemas informáticos, interceptación ilegal de datos y abuso de mecanismos y dispositivos informáticos.

Sostengo que la seguridad informática es el bien jurídico protegido, a partir de los siguientes argumentos:

a) El Tribunal Constitucional peruano reconoce que la tipificación de una conducta como delito solo es válida si "tiene como propósito la protección de bienes jurídicos constitucionalmente relevantes frente a su lesión o puesta en peligro. En otros términos, solo la defensa de un derecho, principio o un interés constitucionalmente relevante podrá justificar en sede penal la restricción en el ejercicio de un derecho fundamental"[328]. No obstante, este pronunciamiento debe ser leído junto aquel en el que desarrolla la relación del Derecho Penal y la Constitución, ya que años antes se indicaba que esta restricción es válida si "tiene como propósito la protección de bienes jurídicos constitucionalmente relevantes (principio de lesividad). Como resulta evidente, solo la defensa de un valor o interés constitucionalmente relevante podría justificar la restricción en el ejercicio de un derecho fundamental"[329]. De esta forma, al aproximarnos a cada delito, nuestra labor será identificar (i) un derecho, (ii) un principio, (iii) un interés o (iv) un valor constitucionalmente relevante que justifique el reproche

326 *Ibid.*, p. 246.

327 Algunos autores utilizan las expresiones *seguridad digital* o *ciberseguridad* para referirse a este término. Toda vez que no existe consenso en doctrina, utilizaré la expresión *seguridad informática*.

328 Tribunal Constitucional del Perú. Sentencia recaída sobre el Exp. N.º 006-2014-PI/TC del 5 de marzo del 2020. F.J. 42.

329 Tribunal Constitucional del Perú. Sentencia recaída sobre el Exp. N.º 019-2005-PI/TC del 21 de julio del 2005. F.J. 35.

penal. Esto nos permitirá descartar algunas propuestas de protección o delimitarlas adecuadamente.

Tomando este marco como referencia, discrepo parcialmente del Dr. Felipe Villavicencio Terreros, reconocido jurista peruano, cuando afirma que "el bien jurídico tutelado en los delitos informáticos se concibe en los planos de manera conjunta y concatenada; en el primero, se encuentra la *información* de manera general (información almacenada, tratada y transmitida mediante los sistemas de tratamiento automatizado de datos), y en el segundo plano, los demás bienes afectados". Coincido con el profesor Villavicencio cuando identifica que los ataques afectan más de un bien jurídico a la vez, pero no cuando señala que el bien jurídico es la *información de manera general*, pues no tiene la calidad de derecho, principio o interés constitucionalmente protegido. Sí, en algunos casos, la información puede ser objeto de delito, pero no el bien jurídico protegido.

De otro lado, de la lectura literal del artículo 1 LDI pareciera que se elevan los sistemas y datos informáticos a *bienes jurídicos de relevancia penal*, sin embargo, dichos bienes intangibles también son objetos delictivos, pero no satisfacen el requisito de ser derechos, principios o intereses constitucionalmente relevantes. No protegemos los datos y sistemas informáticos *per se*, sino su relación y utilidad con los seres humanos o las instituciones -sobre lo cual, regresaré más adelante-.

> En suma, plantear que los delitos informáticos tutelan un bien jurídico específico, propiamente informático, tiene sentido cuando esos delitos, además de incidir en el soporte lógico de un sistema informático, implican el uso de redes computacionales. Algo similar ocurre respecto de los delitos que afectan la funcionalidad del tráfico rodado, cuya existencia no se explica porque se ejecute un comportamiento "mediante" o "respecto de" un vehículo motorizado. Lo relevante, en ese caso, es la conducción de un vehículo en una red de tráfico vial, en cuyo contexto puedan surgir particulares riesgos para la vida, salud o propiedad de cualquiera de las personas que intervienen en ella[330].

330 Mayer Lux, "El bien jurídico protegido en los delitos informáticos", cit., p. 249.

b) La *seguridad ciudadana* es un ejemplo de bien constitucionalmente relevante[331]. Para comprender por qué la *seguridad informática* se erige como bien jurídico es importante sentar una base previa y recordar el desarrollo jurisprudencial que el Tribunal Constitucional ha efectuado sobre la seguridad ciudadana. En el 2005, si bien reconoció que no existe una aproximación conceptual precisa, la conceptualizó en los siguientes términos:

> [...] un estado de protección que brinda el Estado y en cuya consolidación colabora la sociedad, a fin de que determinados derechos pertenecientes a los ciudadanos puedan ser preservados frente a situaciones de peligro o amenaza, o reparados en caso de vulneración o desconocimiento. Derechos como la vida, la integridad, la tranquilidad, la propiedad o la libertad personal suelen ser los principales referentes que integran el contenido de la seguridad ciudadana en atención a lo que el Estado y la colectividad se espera, siendo evidente que, por sus alcances, se trata fundamentalmente de un bien jurídico de relevancia antes que de un atributo o libertad a título subjetivo [...]. En el Estado Social de Derecho, por otra parte, es incuestionable la existencia de roles vitales en torno a la consecución de grandes objetivos. Vista la seguridad ciudadana como uno de esos roles en los que todo Estado se compromete, no cabe discusión alguna en torno del papel relevante que le toca cumplir y la especial posición que el ordenamiento constitucional le suele otorgar[332].

Vivimos en la sociedad de la información en la que no se instalan rejas o tranqueras, pero sí antivirus, cortafuegos y contraseñas; en la que no se necesita desplazarse físicamente para realizar una transferencia económica, pues basta entrar a una página web o instalar una aplicación; en la que no cerramos las puertas y ventanas de nuestros hogares o empresas para mantener al margen a visitantes no deseados, pero sí empleamos medidas de seguridad para que no ingresen

331 Agradezco al jurista y amigo Luciano López Flores, pues sus comentarios me brindaron una perspectiva constitucional más amplia del tema que intento demostrar.

332 Tribunal Constitucional del Perú. Sentencia recaída sobre el Exp. N.º 5994-2005-PHC/TC del 29 de agosto del 2005. F.J. N.º 14 y s.

a nuestros dispositivos y sistemas. La proliferación de las TIC ha generado un gran avance, pero también ha aumentado el riesgo en la navegación. Los bienes jurídicos protegidos encuentran potenciales amenazas y el Estado debe proteger a sus habitantes para que continúen disfrutando a través de su pleno ejercicio.

De otro lado, en el 2012, el Tribunal Constitucional analizó la instalación de rejas metálicas en la vía pública, justificando la restricción a la libertad de tránsito "tras la necesidad de garantizar que la colectividad no se vea perjudicada en sus derechos más elementales frente al entorno de inseguridad recurrente en los últimos tiempos"[333]. De manera análoga, el Estado y los particulares pueden adoptar medidas de protección en los entornos digitales para proteger distintos bienes jurídicos, es decir, resguardar su seguridad digital.

En esta línea, aunque con una propuesta algo distinta sobre el bien jurídico protegido, Laura Mayer sostiene:

> La informática, esto es, la ciencia del almacenamiento, tratamiento y transferencia automatizados de la información cumple diversas funciones de gran relevancia para los individuos. En la actualidad, son muchas las actividades que implican almacenamiento, procesamiento o transferencia de datos a través de sistemas informáticos, y que van desde el uso doméstico, pasando por una serie de servicios, hasta llegar a operaciones de orden económico, gubernamental o militar. Más aún, existen ámbitos como la banca, en que las operaciones que recurren a la informática se han generalizado y han restado absoluto protagonismo a las que se realizan a través de medios tradicionales. Sobre esa base, no es casual que se sostenga que para la economía, la administración y la sociedad en general, internet y otras redes computaciones tienen una importancia equivalente a la de las redes de autopistas, de distribución eléctrica o de abastecimiento de agua[334].

333 Tribunal Constitucional del Perú. Sentencia recaída sobre el Exp. N.º 04094-2011-PA/TC del 23 de enero del 2012. F.J. N.º 4.

334 Mayer Lux, "El bien jurídico protegido en los delitos informáticos", cit., p. 251.

c) En esta línea, frente a las amenazas que ponen en riesgo diversos bienes jurídicos, la *seguridad* informática[335] ha sido reconocida normativamente en el Decreto Legislativo N.° 1412 del 2 de setiembre del 2018 o ley de gobierno digital. Así, en el artículo 30 define la seguridad digital como:

> El estado de confianza en el entorno digital que resulta de la gestión y aplicación de un conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad nacional y los objetivos nacionales en dicho entorno. Se sustenta en la articulación con actores del sector público, sector privado y otros quienes apoyan en la implementación de controles, acciones y medidas.

Algunos años más tarde se promulgó su reglamento mediante Decreto Supremo N.° 029-2021-PCM, del 19 de febrero de 2021, en cuyo artículo 95 se establecen los principios del marco de seguridad digital del estado peruano:

i. Seguridad desde el diseño[336]

ii. Gestión de riesgos[337]

---

335 La Unión Internacional de Telecomunicaciones emplea el término *ciberseguridad*. Así, en la recomendación X.1205, de abril del 2008, la define como "el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/las aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades de seguridad incluyen una o más de las siguientes: disponibilidad; integridad, que puede incluir la autenticidad y el no repudio; confidencialidad".

336 Los servicios digitales se diseñan y crean atendiendo las necesidades de disponibilidad, integridad y confidencialidad de los datos e información que capturan, procesan y distribuyen.

337 La gestión de riesgos de seguridad en el entorno digital está integrada en la toma de decisiones, diseño de controles de seguridad en los servicios digitales y procesos de la

iii. Colaboración y cooperación[338]

iv. Participación responsable[339]

v. Protección de datos e información[340]

vi. Enfoque nacional[341]

vii. Enfoque integral[342]

d) Dicho esto, la seguridad informática no se erige como el bien jurídico protegido por todos los delitos previstos en la LDI, pero sí como un bien constitucionalmente relevante que permitirá adoptar decisiones para salvaguardar otros bienes y derechos que les asisten a las personas y a las instituciones. Estas decisiones pueden ser: sistematizar los delitos afines y que sí protegen exclusivamente este bien jurídico, aumentar o disminuir la pena de los delitos previstos en la LDI, ampliar o reducir las facultades de investigación policial y fiscal en los entornos digitales, regular adecuadamente nuevas instituciones que permitan mejorar la protección de los espacios virtuales, entre otros.

---

entidad. Es responsabilidad de la alta dirección dirigirla, mantenerla e incorporarla en la gestión integral de riesgos de la entidad.

338 Se promueve el intercambio de información, mejores prácticas y experiencias a fin de identificar y prevenir riesgos de seguridad digital; así como detectar, responder y recuperarse ante incidentes en el entorno digital que afecten la continuidad de las entidades, bienestar de las personas y el desarrollo sostenible del país.

339 El Estado y la sociedad en su conjunto tienen responsabilidad en la protección de sus datos personales y gestión de riesgos en el entorno digital, en función de sus roles, contexto y su capacidad de actuar, teniendo en cuenta el impacto potencial de sus decisiones con respecto a otros.

340 Se promueve la implementación de medidas y controles de seguridad organizativos, técnicos y legales para preservar la disponibilidad, integridad y confidencialidad de los datos e información que capture, procese, almacene y distribuya una entidad, así como en cualquier otra forma de actividad que facilite el acceso o la interconexión de los datos.

341 La Seguridad Digital es un componente de la seguridad nacional, respalda el funcionamiento del Estado, la sociedad, la competitividad, la economía y la innovación.

342 La Seguridad Digital es entendida como un proceso integral y holístico constituido por todos los elementos técnicos, humanos, materiales y organizativos relacionados con una entidad.

e) El profesor Luis Miguel Reyna Alfaro, hace dos décadas, postulaba provisionalmente que la información se erige como el bien jurídico protegido de este tipo de delitos. Coincido con sus argumentos, pues es afín a la que se ha desarrollado en estas líneas:

> En base a lo expuesto y acogiéndonos a la clasificación hecha por Adamski es que vamos a abordar el análisis de las conductas lesivas al bien jurídico propuesto. Adamski ha creado más conveniente analizar los atentados contra la "información" a partir de las propiedades que les son inminentes: confidencialidad, integridad y disponibilidad.
>
> La confidencialidad y la integridad de la información son propiedades referidas, básicamente, a impedir la revelación, alteración o delación de la información contenida en ficheros de ordenador. La confidencialidad de la información cobra sus matices más importantes, por ejemplo, en el ámbito de la información médica, estrategias mercantiles, investigaciones científicas, entre otros. En cambio, la integridad resulta vital en el control de tráfico aéreo, la transferencia electrónica de fondos, etc.
>
> Por otra parte, la disponibilidad de la información resulta ser el atributo más importante de los servicios comerciales que dependen de la información, actividades como el "*spamming*" o el "*electronic-mail bombing*" [sic] pueden generar que el disco duro del sistema de información afectado se bloquee y deje de operar.
>
> En este orden de ideas, los ilícitos informáticos pueden ser clasificados en a) conductas lesivas a la confidencialidad de la información, b) conductas lesivas a la integridad de la información, y, c) conductas lesivas a la disponibilidad de la información [...][343]

f) Finalmente, considero importante destacar la posición de la profesora Mayer, pues propone la *funcionalidad informática* como bien jurídico protegido. Considera que la seguridad informática no logra explicar completamente el injusto involucrado en los delitos informáticos que implica el uso de redes computacionales. De este modo, sostiene que "antes de seguros, los sistemas informáticos

343 Reyna Alfaro, Luis. *Los delitos informáticos: Aspectos criminológicos, dogmáticos y de política criminal*. Lima: Jurista, 2002, pp. 245 y s.

deben ser eficientes y eficaces, esto es, capaces de realizar (adecuadamente) las operaciones de almacenamiento, procesamiento o transferencia de datos. En ese sentido, la seguridad informática posibilita que las personas dispongan de sus bienes jurídicos a través de sistemas informáticos eficientes y eficaces. La idea de seguridad informática contribuye a explicar el injusto de los delitos informáticos que suponen el empleo de redes computacionales, en la medida en que actúa como cualidad de un sistema informático eficiente y eficaz"[344].

Sobre este punto, considero que su planteamiento es muy enriquecedor, sin embargo, adoptar dicha posición limitaría el objeto de protección al funcionamiento mismo, dejando de lado algunos delitos íntimamente relacionados. Por ejemplo, en el acceso ilícito no se afecta el funcionamiento, sino la confidencialidad. Sucederá lo mismo con la interceptación ilegal de datos informáticos. En esta misma línea, reconocer la seguridad informática como bien jurídico protegido -y no solo la funcionalidad- permite adelantar la barrera punitiva y sancionar el abuso de mecanismos y dispositivos informáticos.

4.7. ELEMENTOS DE LA SEGURIDAD INFORMÁTICA Y ACTIVIDAD DELICTIVA

El artículo 1 resalta que la finalidad de la LDI es "garantizar la lucha eficaz contra la ciberdelincuencia"; entonces, ¿por qué se denominó *Ley de Delitos Informáticos* y no *Ley de la Ciberdelincuencia* o *de la Cibercriminalidad*? Ciertamente, nuestros legisladores no promovieron mayor debate sobre el nombre que debía recibir este cuerpo normativo, pese a que el proyecto de Ley N.º 2520/2012 proponía una mejor denominación: *Ley de represión de la cibercriminalidad.* Se optó por la recomendada en el proyecto de Ley N.º 34/2011: *Ley de los Delitos Informáticos.*

Como ya he detallado en esta publicación, no existe consenso en la denominación que engloba el fenómeno delictivo aquí estudiado, pues re-

344 Mayer Lux, "El bien jurídico protegido en los delitos informáticos", cit., p. 252.

cibe múltiples denominaciones: *cibercrimen, ciberdelito, cibercriminalidad, ciberdelincuencia, criminalidad informática, delito informático,* etcétera[345]. Sin embargo, algunos especialistas sí diferencian las expresiones *delito informático* y *cibercrimen*[346], tomando como eje central tanto el momento en que empezó a emplearse como el medio u objeto de su comisión.

Como se mencionó en la introducción de esta obra, el concepto de *delito informático* comenzó a emplearse en la década de los setenta para describir los ilícitos vinculados con la informática, ya sea como medio o como objetivo del delito. En el contexto de este estudio, se observa que en nuestro país dicho término se asocia a la Ley N.º 30096, también conocida como LDI.

El término *ciberdelito,* también referido como *cibercrimen* o *ciberdelincuencia,* ha ganado popularidad desde la década de los noventa, derivado del anglicismo *cybercrime*. Esta palabra está compuesta por el prefijo *cyber,* que a su vez proviene de *cyberspace,* un concepto introducido por el escritor de ciencia ficción William Gibson -como se explicó al inicio de la obra-. A diferencia de los delitos informáticos, que abarcan un espectro más amplio, el ciberdelito se centra específicamente en el uso de internet y las Tecnologías de la Información y Comunicación (TIC). En este sentido, una definición amplia de cibercrimen lo describe como "aquel delito cuya característica esencial es el rol central que las TIC juegan en su comisión". Desde el ámbito legislativo, uno de los principales referentes internacionales en la materia es el Convenio de Budapest o Convenio sobre la Ciberdelincuencia, al cual nuestro país se ha adherido y que constituye un pilar fundamental para el desarrollo de este estudio.

Luego de haber efectuado este breve repaso conceptual, he de indicar que la seguridad informática tiene tres elementos centrales. Se les conoce como el trinomio CIA, por sus siglas en inglés: Confidencialidad (*confidentiality*), Integridad (*integrity*) y Disponibilidad (*available*) [347]:

---

345 Miró Llinares, *El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio,* cit., p. 33.

346 Miró Llinares, *El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio,* cit., pp. 33-45; Gil Gil/Hernández Berlinches, *Cibercriminalidad,* cit., pp. 154-156; Barrio Andrés, *Delitos 2.0. Aspectos penales, procesales y de seguridad de los ciberdelitos,* cit., pp. 33-38.

347 Para la elaboración de las definiciones que se exponen a continuación, empleo tanto el Real Decreto 3/2010, del 8 de enero, por el que se regula el Esquema Nacional

> El triángulo confidencialidad, integridad y disponibilidad (CIA TRIAD, en inglés), configura el modelo que explica los alcances del campo de la seguridad informática. Aquel triángulo alude a los conceptos fundamentales para la seguridad informática o, mejor explicado, a tres propiedades que poseen los datos y la información almacenados, transmitidos o recibidos en dispositivos informáticos[348].

A continuación, definiremos cada elemento, ya que los cinco delitos analizados en este libro guardan una estrecha relación, en mayor o menor medida, con estos tres elementos.

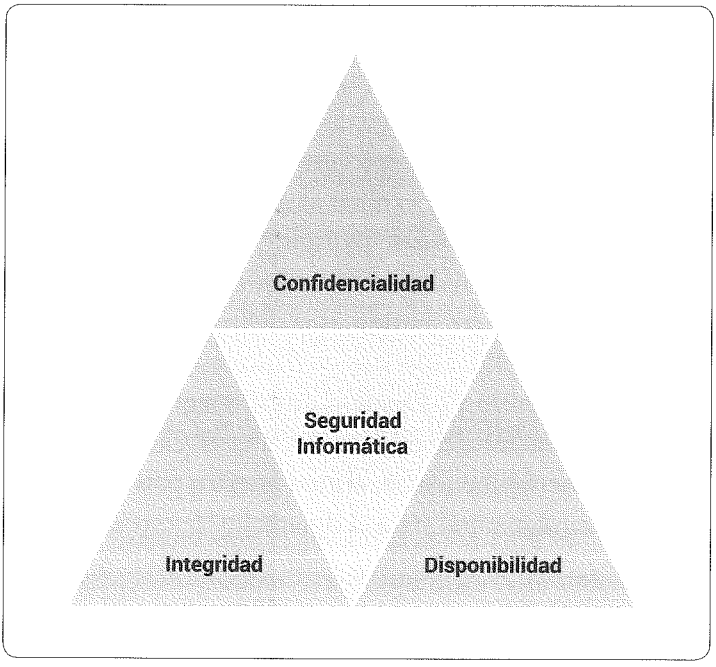


Diagrama 4. Trinomio CIA, por sus siglas en inglés. Elementos de la seguridad informática. Elaboración propia.

de Seguridad en el ámbito de la Administración Electrónica de España como los Términos y definiciones recogido en la Política Nacional de Ciberseguridad del Perú.

348 Brodowski, *Cibercrimen y protección de la seguridad informática,* cit., p. 157.

4.7.1. Confidencialidad

Es la característica consistente en que la información no se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. Así, se garantiza que dicha información sea accesible solo a aquellos usuarios autorizados a tener acceso a la misma.

> La confidencialidad implica que la información es accesible únicamente por el personal autorizado. Es lo que se conoce como *need-to-know*. Con este término se hace referencia a que la información solo debe ponerse en conocimiento de las personas, entidades o sistemas autorizados para su acceso. Ejemplo de falta de confidencialidad son el robo de información confidencial por parte de un atacante a través de Internet, la divulgación no autorizada a través de las redes sociales de información confidencial o el acceso por parte de un empleado a información crítica de la compañía ubicada en carpetas sin permisos asignados, a la que no debería tener acceso[349].
>
> La confidencialidad consiste en garantizar que solo las personas y entidades autorizadas pueden acceder a los datos. Si los delincuentes roban tu número de tarjeta de crédito, se trata de un ataque a la confidencialidad[350].
>
> Mantener los datos, las identidades de los participantes o los sistemas accesibles únicamente para usuarios autorizados. Esto generalmente se logra mediante encriptación [Traducción propia][351].

4.7.2. Integridad

Es la característica consistente en que el activo de información no ha sido alterado de manera no autorizada. De este modo, se salvaguarda la exactitud y totalidad de la información, así como sus métodos de procesamiento.

---

349 Instituto Nacional de Ciberseguridad. *Protección de la información*, p. 6. https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_proteccion-de-la-informacion.pdf

350 Crawley, *Cultura hacker de la A a la Z. Una guía divertida de las personas, ideas y artefactos que han construido el mundo de la tecnología*, cit., p. 267.

351 Brown, Thompson. *Essential guide to cybersecurity for beginners and experts: An elementary plan to protect your family and business form cybercrime*. Independently Published. 2021. [Kindle]

> La integridad de la información hace referencia a que la información sea correcta y esté libre de modificaciones y errores. La información ha podido ser alterada intencionadamente o ser incorrecta y nosotros podemos basar nuestras decisiones en ella. Ejemplos de ataques contra la integridad de la información son la alteración malintencionada en los ficheros del sistema informático mediante la explotación de una vulnerabilidad, o la modificación de un informe de ventas por un empleado malintencionado o por error humano[352].
>
> La integridad consiste en garantizar que solo las personas y entidades autorizadas pueden alterar o modificar los datos. Por ejemplo, puedes configurar tu cuenta en un sistema operativo para lanzar ciertas aplicaciones al iniciar el sistema operativo. He configurado mi copia de Windows 11 para ejecutar Steam, Firefox y LibreOffice cuando lo inicio. Si un ciberatacante modifica la petición de Windows en mi disco duro para que mi cuenta de Windows también inicie su desagradable *malware*, eso es un ataque a la integridad[353].
>
> Asegurarse o verificar que los datos no hayan sido objeto de cambios indebidos o no autorizados. Esto también incluye la verificación del origen de los datos. La integridad no se limita únicamente a los datos, sino que también se aplica a las identidades y a la funcionalidad de los sistemas. La integridad se logra con frecuencia mediante el uso de herramientas criptográficas como las firmas digitales [Traducción propia][354].

4.7.3. Disponibilidad

Es la característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. Permite garantizar que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo deseen.

> La disponibilidad de la información hace referencia a que la información esté accesible cuando la necesitemos. Algunos ejemplos de falta de

352 Instituto Nacional de Ciberseguridad, *Protección de la información*, cit., p. 6.

353 Crawley, *Cultura hacker de la A a la Z. Una guía divertida de las personas, ideas y artefactos que han construido el mundo de la tecnología*, cit., p. 267.

354 Brown, *Essential guide to cybersecurity for beginners and experts: An elementary plan to protect your family and business form cybercrime*, cit.

disponibilidad de la información son: cuando nos es imposible acceder al correo electrónico corporativo debido a un error de configuración [sic], o bien, cuando se sufre un ataque de denegación de servicio, en el que el sistema "cae" impidiendo accesos ilegítimos. Ambos tienen implicancias serias para la seguridad de la información[355].

La disponibilidad consiste en garantizar que los datos son accesibles cuando las entidades y personas autorizadas necesitan utilizarlos. Por ejemplo, desde la década de 2000 hasta aproximadamente 2015, los atacantes solían utilizar *ransomware* que encriptaba de manera maliciosa los datos en el disco duro de la víctima u otro almacenamiento de datos. El atacante, que tenía la clave de desencriptado, extorsionaba a su víctima exigiéndole que pagara sumas de dinero enormes para recuperar sus datos. Eso es un ataque a la disponibilidad[356].

Mantener un sistema en funcionamiento y accesible para sus usuarios, o garantizar que ciertos datos estén disponibles para usuarios autorizados. Esto se logra mediante una variedad de técnicas, como cortafuegos, sistemas de detección y prevención de intrusiones, defensas contra ataques de denegación de servicio (DoS), entre otros. Cabe destacar que la disponibilidad también abarca la calidad del servicio. El sistema no solo debe estar disponible, sino que también debe ofrecer un buen nivel de calidad en el servicio a sus usuarios [Traducción propia][357].

355 Instituto Nacional de Ciberseguridad [España]. *Protección de la información.* https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_proteccion-de-la-informacion.pdf

356 Crawley, *Cultura hacker de la A a la Z. Una guía divertida de las personas, ideas y artefactos que han construido el mundo de la tecnología*, cit., p. 267.

357 Brown, *Essential guide to cybersecurity for beginners and experts: An elementary plan to protect your family and business form cybercrime*, cit.

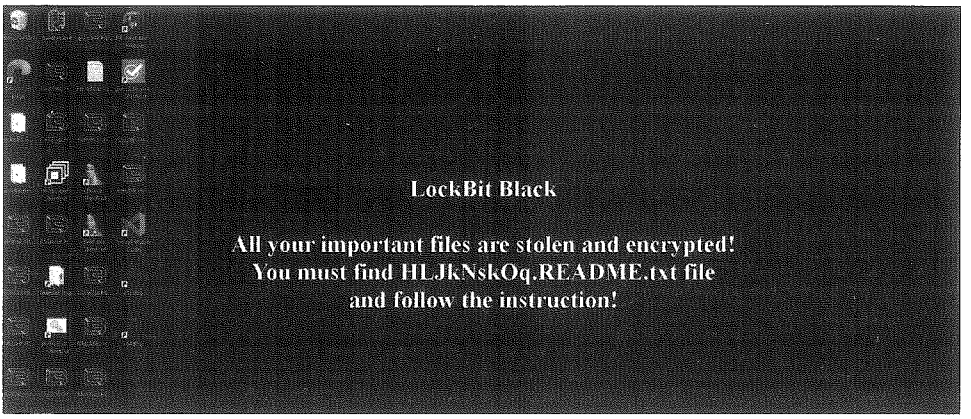


Imagen 9[358]. El *ransomware* LockBit 3.0 encripta archivos, les cambia de nombre y varía el fondo de pantalla de la víctima. Entre mayo y agosto del 2023, infectó más de 60 millones de dispositivos.

Los elementos que integran la seguridad informática permiten sistematizar o agrupar cinco delitos informáticos, según el objeto principal de vulneración o ataque:

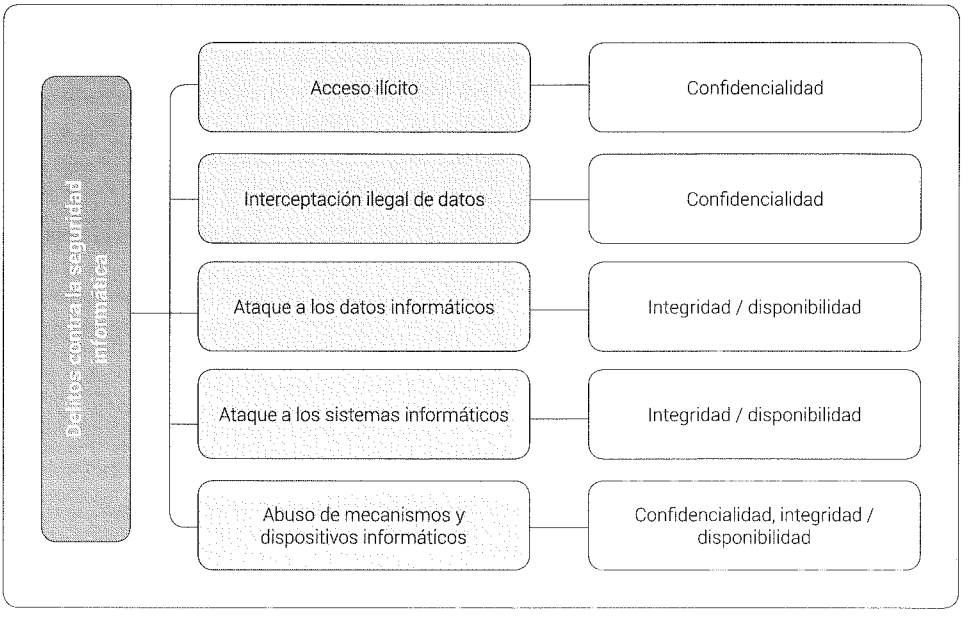


Diagrama 5. Relación de los delitos informáticos con los principales elementos de la seguridad informática que afectan. Elaboración propia.

358 La imagen fue descargada de: TX ONE NETWORK. *LockBit 3.0 Analysis: How to Enhance Ransomware and Malware Protection*, publicado el 18 de abril de 2023. Disponible en: https://www.txone.com/blog/malware-analysis-lockbit-3-0/

Como se puede apreciar, cada delito afecta principalmente, un elemento de la seguridad informática. Esto no quiere decir que no se puedan afectar otros elementos de forma simultánea, sino que es posible reconocer uno de ellos como el eje central de protección. Algunos ejemplos ayudarán a desarrollar esta idea:

- En el delito de acceso ilícito, se sanciona el ataque a la confidencialidad; sin embargo, en algunos casos podría comprometerse su integridad: piénsese en un *malware* que modifica la configuración del sistema para que el atacante pueda ingresar a este.
- En la interceptación ilícita de datos, el atacante podría instalar un *software* malicioso para lograr su objetivo; pese a ello, lo que se protege es el ataque a la confidencialidad antes que su integridad.
- En algunos casos de atentados contra los sistemas informáticos, el atacante puede haber accedido a los sistemas empleando la contraseña del administrador; no obstante, el objeto central de protección será la integridad que ha sido mermada por el ciberataque.
- En el delito de abuso de mecanismos y dispositivos informáticos, el legislador ha anticipado la barrera punitiva para castigar aquellas conductas que potencialmente puedan dañar la confidencialidad, la integridad o la disponibilidad de los datos y los sistemas informáticos.

4.8. ACTUACIÓN DELIBERADA E ILEGÍTIMA

La Ley N.º 30171 del 10 de marzo del 2014 agregó los términos *deliberada* e *ilegítimamente* a seis de los diez delitos que contempla actualmente la Ley N.º 30096: acceso ilícito (art. 2), atentado contra la integridad de datos informáticos (art. 3), atentado contra la integridad de sistemas informáticos (art. 4), interceptación de datos informáticos (art. 7), fraude informático (art. 8) y abuso de mecanismos y dispositivos informáticos (art. 10). Este cambio tiene como génesis el proyecto de Ley N.º 2991/2013 del congresista Juan Carlos Eguren. En la exposición de motivos, el autor expresamente señala que la Ley N.º 30096 no cumple los estándares previstos en el Convenio sobre la Ciberdelincuencia al no haber incluido en estos seis delitos "la calidad de deliberada e ilegítima de la conducta". El proyecto de Ley N.º 2999/2013 del congresista Mauricio Mulder recogió la misma propuesta. En menor medida, se sumó el proyecto de Ley

N.º 3105/2013 del grupo parlamentario Perú Posible, que únicamente propuso agregar la expresión *ilegítima* al delito de atentado contra la integridad de datos informáticos.

Por esta razón, actualmente, en los cinco delitos mencionados, la conducta desplegada debe ser **deliberada e ilegítima**, siguiendo la recomendación prevista en el artículo 2 del Convenio sobre la Ciberdelincuencia: "Cada parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno el acceso deliberado e ilegítimo a todo o parte de un sistema informático". Sin embargo, tomando en consideración la estructura de la teoría del delito que recoge nuestro ordenamiento -tipicidad, antijuricidad y culpabilidad-, el contenido de estos conceptos requiere ser desarrollado para evitar problemas de interpretación y aplicación.

Antes de continuar, debo indicar que la Convención de las Naciones Unidas contra la ciberdelincuencia introduce las expresiones *deliberada* y *sin derecho* para referirse al dolo y a la actuación antijurídica[359].

4.8.1. Actuación deliberada

En primer lugar, debo señalar que el Código Penal peruano recoge solo tres delitos en los que se ha utilizado la expresión *deliberadamente*. Esto nos permitirá tener un marco de referencia para la interpretación que se propondrá más adelante:

Delito	Fórmula legislativa
Secuestro (art. 152 CP)	La misma pena se aplicará al que con la finalidad de contribuir a la comisión del delito de secuestro, suministra información que haya conocido por razón o con ocasión de sus funciones, cargo u oficio, o proporciona **deliberadamente** los medios para la perpetración del delito.

359 Al respecto, ver la **Convención de las Naciones Unidas contra la ciberdelincuencia, art. 7** (acceso ilícito), **art. 8** (interceptación ilícita), **art. 9** (interferencia con datos electrónicos), **art. 10** (interferencia con un sistema de tecnología de la información y las comunicaciones), **art. 11** (uso indebido de dispositivos), **art. 12** (falsificación relacionada con un sistema de tecnología de la información y las comunicaciones), **art. 13** (robo o fraude relacionados con un sistema de tecnología de la información y las comunicaciones), **art. 14** (delitos relacionados con material en línea que muestra abusos sexuales de niños o explotación sexual de niños), **art. 15** (instigación o captación con el fin de cometer un delito sexual contra un niño) y **art. 16** (difusión no consentida de imágenes de carácter íntimo).

Delito	Fórmula legislativa
Atentado contra la seguridad y salud en el trabajo (art. 168-A CP)	El que, **deliberadamente**, infringiendo las normas de seguridad y salud en el trabajo y estando legalmente obligado, ponga en peligro inminente la vida, salud o integridad física de sus trabajadores de forma grave, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años. Si, como consecuencia de la inobservancia **deliberada** de las normas de seguridad y salud en el trabajo, se causa la muerte del trabajador o terceros o le producen lesión grave, y el agente pudo prever este resultado, la pena privativa de libertad será no menor de cuatro ni mayor de ocho años en caso de muerte y, no menor de tres ni mayor de seis años en caso de lesión grave.
Extorsión (art. 200 CP)	200.3 La pena establecida en el párrafo 200.1 se aplicará al que, con la finalidad de contribuir a la comisión del delito de extorsión, suministra información que haya conocido por razón o con ocasión de sus funciones, cargo u oficio o proporciona **deliberadamente** los medios para la perpetración del delito.

Cuadro 12. Cuadro resumen de los delitos que recogen el elemento *deliberadamente* en el Código Penal.

En segundo lugar, si acudimos a una interpretación literal, tendremos que una conducta será **deliberada** cuando sea intencional, voluntaria, o hecha a propósito. Es más, si accedemos a la versión oficial del Convenio de Budapest, redactada en inglés, veremos que los delitos bajo análisis incluyen el elemento *intentionally* en la siguiente fórmula:

> Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, **when committed intentionally** [...] [El resaltado es mío].

Entonces, ¿por qué se incluyó la expresión deliberadamente o *intentionally* en el Convenio de Budapest? Porque se quiso investigar y sancionar aquella conducta dolosa, descartando, de este modo, actuaciones culposas o negligentes.

En tercer lugar, la interpretación propuesta se ve confirmada si analizamos cómo se utiliza o desarrolla la expresión *deliberada* en el Informe Explicativo del Convenio sobre la Ciberdelincuencia:

> 39. **Todos los delitos contenidos en el Convenio deben ser cometidos de manera deliberada para que se aplique la responsabilidad penal.** En ciertos casos, un elemento deliberado específico forma parte del delito. Por ejemplo, en el Artículo 8 que trata del delito de fraude informático, la intención de obtener un beneficio económico es un elemento constitutivo del delito. Quienes redactaron el Convenio llegaron al acuerdo de que **el significado**

> **exacto del término "deliberado" debería ser interpretado conforme a las leyes de cada país.**
>
> [...]
>
> 70. [Ataques a la integridad del sistema] El delito debe ser cometido de manera deliberada; **ello quiere decir que quien lo comete debe tener la intención** de causar una obstaculización grave[360].

Siendo esto así, el término *deliberado* se encuentra íntimamente ligado al ámbito subjetivo del delincuente. Por esta razón, considero que el Convenio de Budapest emplea la expresión *deliberada* para establecer conductas dolosas y diferenciarlas de las culposas o negligentes dado que el citado Convenio no sugiere tipificarlas como delito.

En cuarto lugar, si *deliberadamente* es sinónimo de *dolosamente*, debemos responder la siguiente pregunta: ¿era necesario incluirlo en la tipificación de los diversos delitos recogidos en la Ley de Delitos Informáticos? No. De hecho, su inclusión, en la modificación del 2014, genera problemas de interpretación.

El Código Penal peruano establece en el artículo 12 que "las penas establecidas por la ley se aplican siempre al agente de infracción dolosa. El agente de infracción culposa es punible en los casos expresamente establecidos por la ley". Obviamente, el Convenio de Budapest buscó una fórmula general, ya que su vocación es universal. De ahí que estableciera que las legislaciones locales interpretarían el elemento *deliberadamente*: no ordenó que fuese incluido en su redacción. Prueba de ello es que si se revisa la legislación de los estados latinoamericanos que se han adherido al citado Convenio, ninguno de ellos recoge este elemento en su tipificación.

Lamentablemente, no basta decir que *deliberadamente* equivale a *dolosamente*[361], pues nuestra legislación lo ha recogido como un elemento adicional. De ahí que la doctrina local establezca que este elemento limita las conductas que pueden ser perseguidas a aquellas que se realicen con dolo directo.

---

360 La expresión *deliberadamente* se encuentra también en los parágrafos 58, 59, 63, 69, 70, 71, 76, 88, 90, 105, 108, 113, 121 y 155.

361 En esta posición se encuentra Jiménez Herrera, *Manual de derecho penal informático*, cit., pp. 409, 414, 418, 455 y 491. También, Espinoza Calderón, *Delitos informáticos y nuevas modalidades delictivas*, cit., pp. 74, 78, 84, 93 y 104.

Jorge Vega Aguilar y Maguín Arévalo Minchola, por ejemplo, al analizar el delito de acceso ilícito -que incluye el elemento *deliberadamente-*, sostienen que "el tenor típico exige obligatoriamente que el hecho haya sido realizado de forma deliberada, esto es, con conocimiento y voluntad integral del hecho. Esto implicaría la exigencia de dolo directo para la imputación del delito de acceso ilícito"[362].

En la misma línea, el profesor Eduardo Oré Sosa analiza el elemento subjetivo de dos delitos de la LDI:

> En cuanto al aspecto subjetivo, el legislador exige que el acceso ilícito sea deliberado. Esto suele entenderse como dolo directo. Se trata de un requisito que en modo alguno restringe el ámbito de la aplicación del tipo, pues la necesidad de que se vulnere una específica medida de seguridad torna irrelevante tal exigencia[363].
>
> En este delito [atentado a la integridad de sistemas informáticos] se exige también un comportamiento deliberado. No obstante, más que acreditar un *animus nocendi* o intención de dañar, lo que se debe imputar es el conocimiento de la potencialidad lesiva de la conducta, esto es, la posibilidad de que se produzca el resultado de inutilización o entorpecimiento[364].

García León, por su parte, sigue esta misma posición al analizar el delito de acceso ilícito -antes de la modificación del 2023-:

> El delito de acceso ilícito es un delito eminentemente doloso, el agente tiene que conocer que accede de forma ilegítima sin tener la titularidad, autorización o administración del sistema, pues para ello vulnera las medidas de seguridad que le impiden ese libre acceso.
>
> Ahora bien, la expresión deliberadamente importa la intención del legislador que este delito solo pueda ser cometido mediante dolo y dolo

362 Arévalo Minchola/Vega Aguilar, *Ciberdelitos. Análisis en el sistema penal*, cit., pp. 262 y s.

363 Oré Sosa, Eduardo. *Delictum. Apuntes de derecho penal.* Lima: Editores del Centro, 2022, p. 193.

364 Oré Sosa, *Delictum. Apuntes de derecho penal*, cit., p. 196.

> directo o de primer grado, es decir, que el agente tenga pleno conocimiento que su actuar es ilegítimo, lo que daría mínimas posibilidades a errores o a riesgos de atipicidad subjetiva de la conducta[365].

En quinto lugar, debo indicar que, a nivel legislativo, nuestro ordenamiento tiene una propuesta represiva dispar ya que, si revisamos la LDI, veremos que solo algunos tipos penales exigen que la conducta sea deliberada y otros no. Desde el punto de vista técnico, no tiene mayor fundamento ni explicación:

Delito	¿Exige que la conducta sea deliberada?
Acceso ilícito (art. 2 LDI)	Sí
Atentado a la integridad de datos informáticos (art. 3 LDI)	Sí
Atentado contra la integridad de sistemas informáticos (art. 4 LDI)	Sí
Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos (art. 5 LDI)	No
Chantaje sexual con materiales elaborados o modificados por medios digitales o tecnológicos (art. 5-A LDI)	No
Interceptación de datos informáticos (art. 7 LDI)	Sí
Fraude informático (art. 8 LDI)	Sí
Préstamos informáticos extorsivos (art. 8-A LDI)	No
Suplantación de identidad (art. 9 LDI)	No
Abuso de mecanismos y dispositivos informáticos (art. 10 LDI)	Sí

Cuadro 13. Cuadro resumen de los delitos que recogen el elemento deliberadamente en la LDI.

En sexto y último lugar, debo señalar que, desde mi posición, la actual redacción del tipo penal generará dificultades en la etapa intermedia, pues el Ministerio Público deberá describir por qué la conducta imputada es tanto dolosa como deliberada. Este cuestionamiento, como sabrá el lector, se produce en el control formal de la acusación, ya que en ese momento la redacción de la imputación debe desarrollar todos los elementos -tanto objetivos como subjetivos del tipo-. Dicho esto, considero que el elemento deliberado, en efecto, deja de lado toda conducta que opere bajo el dolo eventual, pero no creo que

365 García León, Godofredo André. "Análisis del tipo de acceso ilícito. Bien jurídico, tipicidad objetiva y subjetiva, autoría y participación, y su distinción con el delito de atentado a la integridad de datos y sistemas informáticos". En: Espinoza Calderón, Víctor Raúl (coord.). *Cibercriminalidad y delitos informáticos*. Lima: Instituto Pacífico, 2023, p. 371.

se circunscriba únicamente al dolo directo de primer grado, sino que permite ampliarlo hasta el dolo directo de segundo grado.

En este punto, recomiendo al lector el estudio de la publicación peruana *El dolo como magnitud graduable*, de David Mendiguri Peralta, pues en ella encontrará una revisión detallada y reflexiva de las diferentes tesis y su desarrollo jurisprudencial. Mi publicación, lamentablemente, postula algunas ideas y presenta breves reflexiones. Dicho esto, considero que la expresión *deliberadamente* es un coto al dolo, pues no toda conducta dolosa será castigada:

a. Dolo directo de primer grado.- Siguiendo la clasificación tradicional, se caracteriza "porque la realización del tipo, o del resultado, constituye la finalidad del autor. Aquí el componente volitivo es intencionalidad, en este elemento radica su peso específico y su nivel de realización es el máximo o más alto. El elemento intelectual también puede manifestarse en el más alto grado, es decir, como conocimiento seguro o alto grado de probabilidad [...]"[366].

b. Dolo directo de segundo grado.- También conocido como *dolo de consecuencias necesarias*, "se caracteriza porque el conocimiento está en el más alto grado, eso es, la certeza, la seguridad de la realización del tipo como consecuencia de la acción. En cambio, el elemento volitivo no está en su máxima intensidad, es menos intenso, porque no es el fin principal que persigue, sino que es la consecuencia necesariamente unida a la consecución de aquel fin. Por ir necesariamente unido a su fin, lo integra igualmente en su finalidad"[367].

c. Dolo eventual.- En este escenario, "lo que el sujeto debe prever como posible o como probable (y eventualmente contar con ello) al momento de dar comienzo a su acción no es la producción del resultado, sino la concurrencia de los elementos típicos. De esta manera, si el sujeto al realizar la acción cuenta con la posibilidad

366 Mendiguri Peralta, David Rosario. *El dolo como magnitud graduable: Cómo determinar la pena según la intensidad del dolo. Análisis doctrinario y jurisprudencial.* Lima: Instituto Pacífico, 2024, p. 206.

367 Mendiguri Peralta, *El dolo como magnitud graduable. Cómo determinar la pena según la intensidad del dolo. Análisis doctrinario y jurisprudencial*, cit., p. 209.

> de la realización del tipo, se dará el dolo eventual; si confía en que el tipo no se realice, se dará la imprudencia consciente"[368].

Dicho esto, sostengo que el elemento *deliberadamente* circunscribe las conductas a castigar a aquellas en las que el sujeto activo actúa con dolo directo -sea de primer o segundo grado-, dejando el dolo eventual sin castigo. Una eventual reforma legislativa exige la eliminación de este elemento subjetivo, pues no tiene aporte alguno, sino que genera graves dificultades en la investigación y en la aplicación.

4.8.2. Actuación ilegítima

Finalmente, el término *ilegítimo* alude a la antijuricidad de la conducta. El parágrafo 38 del Informe Explicativo así lo evidencia:

> Una particularidad de los delitos incluidos es el requisito expreso de que la conducta en cuestión sea llevada de manera "ilegítima" [sic]. Esto refleja la idea de que la conducta descrita no siempre es punible *per se*, sino que puede ser legal o justificada, no solo en aquellos casos en los que corresponde aplicar una defensa legal clásica, como el consentimiento, la defensa propia o la necesidad, sino también cuando otros principios o intereses conducen a la exclusión de la responsabilidad penal. El término *ilegítimo* deriva su significado del contexto en que está utilizado. Así, sin restringir la manera en que las Partes pueden aplicar el concepto en su derecho interno, puede referirse a una conducta realizada sin facultades para hacerlo (ya sean de orden legislativo, ejecutivo, administrativo, judicial, contractual o consensual) o a una conducta que no está de otro modo comprendida dentro de las justificaciones, excusas y defensas legales establecidas o los principios pertinentes con arreglo a las leyes nacionales. Por consiguiente, el Convenio no afecta a las conductas legítimas de un gobierno (por ej., cuando el gobierno de una de las Partes interviene para mantener el orden público, proteger la seguridad nacional o investigar delitos penales). Por otra parte, las actividades legítimas y comunes inherentes al diseño de las redes, o legítimas y comunes respecto de las prácticas comerciales no deben ser consideradas delitos. Ejemplos específicos de estos tipos de excepciones se presentan en relación con delitos específicos en el texto correspondiente del Memorando Explicativo

368 *Ibid.*, p. 212.

> que figura más abajo. Queda a criterio de las Partes determinar la manera en que esas exenciones son implementadas en su sistema jurídicos nacionales (conforme al derecho penal o de algún otro modo)[369].

Incluir la voz *ilegítima*, al igual que *deliberada*, no era necesario. Nuestro ordenamiento se encuentra preparado para abordar estos supuestos. Es más, ningún Estado que se adhirió al Convenio de Budapest incluye dicha expresión. Si analizamos los delitos recogidos en la LDI, veremos que no todos incluyen el elemento *ilegítimo* en su construcción, sin que esto signifique que se castigará todo tipo de conductas:

Delito	¿Exige que la conducta sea ilegítima?
Acceso ilícito (art. 2 LDI)	Sí
Atentado a la integridad de datos informáticos (art. 3 LDI)	Sí
Atentado contra la integridad de sistemas informáticos (art. 4 LDI)	Sí
Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos (art. 5 LDI)	No
Chantaje sexual con materiales elaborados o modificados por medios digitales o tecnológicos (art. 5-A LDI)	No
Interceptación de datos informáticos (art. 7 LDI)	Sí
Fraude informático (art. 8 LDI)	Sí
Préstamos informáticos extorsivos (art. 8-A LDI)	No
Suplantación de identidad (art. 9 LDI)	No
Abuso de mecanismos y dispositivos informáticos (art. 10 LDI)	Sí

Cuadro 14. Cuadro resumen de los delitos recogen el elemento *ilegítimamente* en la LDI.

En el ordenamiento penal peruano, la ilegitimidad debe ser analizada en concordancia con el artículo 20 CP, que regula las causas que eximen la responsabilidad penal. Entre ellas: (i) estado de necesidad justificante, (ii) cumplimiento de un deber, (iii) ejercicio legítimo de un derecho, (iv) cumplimiento de orden obligatoria de autoridad competente, (v) ejercicio legítimo de un oficio o cargo y (vi) autorización de la autoridad competente.

Ahora bien, al revisar el diario de debates del 12 de febrero de 2014, en el que se discutió la primera modificación de la LDI, vemos que nuestros legisladores hicieron eco de las preocupaciones periodísticas y de opinión, pero renunciaron al debate jurídico penal esperado:

369 El término *ilegítimo* es desarrollado en los siguientes parágrafos del Informe Explicativo: 47, 48, 58, 59, 62, 68, 76, 77, 81, 88, 89, 103 y 115.

> El señor Eguren Neuenschwander (PPC-APP).- Gracias, señor presidente.
>
> Como los señores parlamentarios recordarán, [se] dio una ley, la Ley 30096, Ley de Delitos Informáticos. Una iniciativa que se convirtió en ley importante, porque nos pone en un escenario de modernidad en la lucha contra la ciberdelincuencia en la serie de modalidades que permanentemente están en proceso de avance, en la medida y en paralelo al avance tecnológico.
>
> Sin embargo, esta ley generó preocupación en muchos de los destinatarios de la norma, fundamentalmente la gente vinculada a las tecnologías de la información y comunicación que no necesariamente son abogados.
>
> En consecuencia, hubo varios artículos que generaron suspicacia, generaron preocupaciones que dio lugar a que se presenten tres proyectos de ley. Los mismos que han sido recogidos mayoritariamente en este dictamen, donde se hace una serie de precisiones para evitar preocupaciones, dudas, suspicacias. Básicamente porque al ser una ley de carácter penal, tiene que estar referida en el marco del Código Penal, y específicamente a la parte del régimen general donde se habla de dolo, daño, **una actitud deliberada, ilegítimamente**, temas que no estaban expresamente señalados en la Ley de Delitos Informáticos, porque se entiende que, al ser una norma penal, está dentro del marco de referencia general [El resaltado es mío].
>
> Sin embargo, repito, estas preocupaciones creo válidas, creo legítimas, han sido recogidas en el proyecto de ley; y les pido a los señores parlamentarios que me puedan acompañar para hacer esta exposición muy didáctica [...]

En esta jornada, se discutió la inclusión del artículo 12 LDI: "Está exento de responsabilidad penal el que realiza las conductas descritas en los artículos 2, 3, 4 y 10 con el propósito de llevar a cabo pruebas autorizadas u otros procedimientos autorizados destinados a proteger sistemas informáticos". Es en este escenario, que se advirtió que el artículo 20 CP excluía diversas conductas al no contravenir el ordenamiento jurídico. Tal y como sostengo en esta publicación, se sostuvo que el artículo 20 CP impide que se castigue cualquier conducta. Lamentablemente, esta opinión no caló en la discusión:

El señor Beingolea Delgado (PPC-APP).- Gracias, presidente.

[...] En todo caso decir que para quien tenga alguna duda al respecto, que la solicitud que he escuchado ya está cubierta por el artículo 20 del Código Penal; **el Código Penal aquí hay que verlo como un todo, solemos no verlo como un todo, vemos el articulito y queremos que ahí estén todas las excepciones y todas las agravantes y todas las exoneraciones, y no es así**, hay excepción de responsabilidad genéricas, ¿no es cierto?, hay inimputabilidades genéricas [El resaltado es mío].

Es decir, por ejemplo, si un menor de edad cometiese un hurto, no tiene el mismo tratamiento que un mayor de edad un niño de ocho años, ¿correcto?, pero eso no lo dice el artículo del hurto, pues lo dice la parte general del Código Penal, porque sería ocioso que lo diga el hurto, en el robo, en el asesinato, sería una cosa ilógica, por eso es que el Código Penal funciona así, hay cuestiones generales.

En el artículo 20 del Código Penal, que son las causas que eximen o atenúan la responsabilidad penal, contempla una serie de figuras, entre otras, la que ahora estaba siendo solicitada para este artículo en particular y me permito leerlo, artículo 20, inciso 8) del Código Penal, dice: "Está exento de responsabilidad el que obra por disposición de la ley, en cumplimiento de un deber o en el ejercicio legítimo de un derecho, oficio o cargo".

Esto, precisamente, por ejemplo, lee un periodista cuando se encuentra frente a un proceso de difamación, por ejemplo, y dice: "Yo difundo esto en el ejercicio legítimo de un derecho, en el ejercicio legítimo de mi oficio de periodista", de manera que eso ya está contemplado en el artículo 20, inciso 8 del Código Penal, no hace preverlo en cada uno de los artículos posteriores de la parte especial del código en donde se delimitan los delitos.

Gracias, presidente.

Coincido con la opinión del congresista Beingolea. Aunque su análisis surge a partir del debate de la incorporación del artículo 12 LDI, se aplica a los elementos *deliberada e ilegítimamente* -aquí analizados-. Dicho esto, una eventual reforma legislativa debe eliminar el término *ilegítimamente* de los tipos penales previamente citados, pues su inclusión no es necesaria y podría generar confusión al interpretarla o aplicarla.

4.9. SER *HACKER* NO SIGNIFICA SER CIBERDELINCUENTE

Los cinco delitos que analizo en esta obra pueden ser cometidos por cualquier ciudadano, pues se enmarcan en la categoría de delitos comunes: Es más, el autor no necesita tener conocimiento técnico especializado. No obstante, como se verá en cada uno de los capítulos siguientes, de manera casi uniforme, la doctrina nacional resalta las cualidades tecnológicas como si se tratara de una característica inherente a este tipo de delincuentes. Incluso, algunos equiparan la condición de *hacker* a la del ciberdelincuente, cuando no son sinónimos.

La academia ha identificado diferentes *generaciones* de *hackers*, según sus motivaciones e intereses.

- Entre fines de los cincuenta e inicios de los sesenta, los *true hackers* fueron los pioneros de la computación y quienes tenían acceso a sistemas disponibles en instituciones como el MTI.
- En la década de los setenta, los *hardware hacker* tuvieron un rol muy importante en la revolución informática gracias a sus aportes para la mejora del *hardware*.
- En la década de los ochenta, los *game hackers* se centraron en el desarrollo de aplicaciones de *software*.
- Finalmente, en los noventa, los *microserfs* -expresión peyorativa que resulta al unir Microsoft y *serfs* (siervos)- fueron reclutados por la industria informática. En tanto los *hacktivists* entremezclaron hackeos con actividades políticas -a veces radicales-[370].

En enero de 1986, Loyd Blankenship, conocido como «The Mentor», publicó un texto conocido como *Hacker Manifiesto* o *La Consciencia de un Hacker* en la séptima edición de la revista *Phrak*. Este texto refleja la curiosidad por el conocimiento y el aprendizaje que caracteriza a esta comunidad, aunque algunos han tratado de justificar actuaciones ilegales bajo estos ideales:

> This is our world now... The world of the electron and the switch, the beauty of the bad. [...] We explore... And you call us criminals. We

370 Lavorgna, Anita. *Cybercrimes. Critical issues in a global context*. Londres: Red Globes Press, 2020, p. 54.

> exist without skin color, without nationality, without religious bias... And you call us criminals. You build atomic bombs, you wage wars, you murder, you cheat, and lie to us and try to make us believe it´s for our own good, yet we´re the criminals.
>
> Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for.
>
> I am a hacker, and this is my manifesto. You may stop this individual, but you can't stop us all[371].

Los ideales de la ética *hacker* han sido resumidos en seis pilares: (1) toda la información debe ser de libre acceso; (2) el acceso a los ordenadores (y a todo aquello que nos puede enseñar algo acerca de cómo funciona el mundo) debe ser ilimitado y total; (3) desconfía de la autoridad, promueve la descentralización; (4) un *hacker* debe ser valorado por sus *hacks*, es decir, por la calidad de sus diseños y programas, no por criterios falsos y postizos como las titulaciones académicas, la raza o la posición social; (5) un *hacker* puede crear arte y belleza con un ordenador; (6) los ordenadores pueden mejorar nuestras vidas[372].

Lamentablemente, a lo largo del tiempo, el término *hacker* ha sido erróneamente asociado con actividades delictivas, lo que ha llevado a una percepción distorsionada de esta comunidad.

---

371 Lavorgna, *Cybercrimes. Critical issues in a global context*, cit., p. 55.

372 Contreras, Paul. *Me llamo Kohfman. Identidad hacker: una aproximación antropológica*. Barcelona: Gedisa, 2004, pp. 33 y s. Algunos autores grafican las múltiples motivaciones que podrían influir en la actuación de esta comunidad: diversión, búsqueda de reconocimiento y liderazgo, socialización, inquietud intelectual, demostración de su inteligencia, ideología antisistema, actos políticos, frustración, interés por los retos y la solución de problemas, acceder a información clasificada, vandalismo, curiosidad, espionaje industrial, extorsión y fraude, exploración, rebeldía y oposición a la autoridad, búsqueda de sensaciones, lucro, aburrimiento, ideal romántico del *hacker*, conseguir atención mediática, ocupación profesional, venganza, defensa de la libertad digital, escapar de la realidad física, sentirse superior, hacktivismo (Torres Blanco, Antoni y otros. "El *hacking* desde una perspectiva legal, criminológica y técnica". En: Garrós Font, Imma *et al. Delitos cibernéticos: amenazas digitales del siglo XXI. Análisis normativo, psicológico y criminológico*. Navarra: Thomson Reuters / Aranzadi, 2023, p. 86).

> Desde un punto de vista criminológico, las motivaciones de los *hackers* son variadas y responden a objetivos diversos. Algunos de ellos van desde la simple *curiosidad*, donde existe la única motivación de espiar contenidos privados ajenos, hasta *fines delictivos*, por ejemplo, para obtener un beneficio económico mediante la comisión de fraudes y estafas a través de la web. Otras motivaciones pueden ser la *malicia*, en tanto deseo de destrucción arbitraria; *motivaciones políticas*, donde determinados activistas o grupos llevan adelante diferentes reclamos o represalias contra grupos de poder o gobiernos; *fines ideológicos*, como los boicots a sistemas comerciales a favor del libre flujo de información; o motivaciones de *seguridad*, básicamente para demostrar las vulnerabilidades de los programas de *software* informáticos y así obligar a las organizaciones o empresas responsables a mejorar la seguridad de los sistemas[373].

De este modo, en la década de los setenta aparece o se construye un nuevo grupo, con fines e ideales mucho más radicales, que no pueden identificarse con la cultura *hacker* en los términos aquí estudiados. Me refiero al *cyberpunk*:

> Los punks cultivaron el nihilismo, el anarquismo, el escepticismo, la ética *do it yourself* y el libre albedrío, cuestionaron las convenciones sociales y la cultura de masas, e hicieron popular el lema "*No future*" [sic], axioma distópico del posmodernismo. Este distopismo es el que adopta el *cyberpunk*, como subgénero de ciencia ficción, a finales de esa década y en los años ochenta del siglo XX, para recrear un futuro próximo oscuro, siniestro, determinado y dominado por la alta tecnología, en el que el ser humano no es más que una rata de laboratorio en manos de grandes corporaciones empresariales transnacionales que han sustituido a los Estado-nación[374].

A continuación, explicaré por qué considerar que delitos como el acceso ilícito, los atentados contra la integridad de datos y los ataques a sistemas informáticos son cometidos por *hackers* no solo es inexacto, sino que, además, puede generar un sesgo en los investigadores (policiales o fiscales), afectando la correcta

373 Sain, Gustavo Raúl. *Delitos y nuevas tecnologías. Fraude, narcotráfico y lavado de dinero por internet*. Buenos Aires: Editores del Puerto, 2012, p. 5.

374 Quian, Alberto. *Civilización hacker*. Madrid: Grupo Anaya, 2022, p. 228.

identificación de los responsables. Este error de percepción también puede influir negativamente en la propia víctima y en su estrategia de defensa legal.

4.9.1. El tratamiento del término *hacker* en los medios de comunicación

Como he indicado en diversos pasajes de esta obra, se suele considerar que quienes cometen delitos informáticos son *hackers*. Sin embargo, esta última denominación ha ensombrecido la labor de los *hackers* bajo el manto del prejuicio, pues se les equipara con los ciberdelincuentes[375].

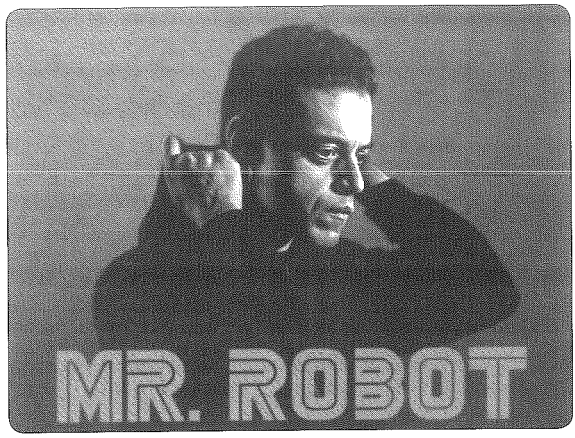


Imagen 10[376]. Las series y películas no solo refuerzan estereotipos sobre la figura del *hacker*, sino que también lo asocian frecuentemente con la comisión de delitos informáticos.

Si tomamos el inicio de la pandemia como punto de referencia, veremos que los medios de comunicación peruanos han reportado distintos ataques cometidos por ciberdelincuentes -accesos ilícitos, atentados contra los datos y

375 A nivel local, el trato sinonímico de *hacker* con ciberdelincuente lo vemos en: "El legislador adelanta las barreras de protección del bien jurídico porque sanciona como delito consumado las conductas de intrusismo sin esperar a que se produzca el último propósito del *hacker* (retiros de dinero de cuentas bancarias, el tráfico de un secreto empresarial o de una información reservada, etc.)" (Oré Sosa, *Delictum. Apuntes de derecho penal*, cit., p. 193). En sentido contrario: "Hacker: Experto en informática capaz de entrar en sistemas cuyo acceso es restringido. No necesariamente con malas intenciones" (Arévalo Minchola/Vega Aguilar, *Ciberdelitos. Análisis en el sistema penal*, cit., p. 520).

376 La imagen fue descargada de: Rottentomatoes. *Mr. Robot*, del 24 de junio del 2015. https://www.rottentomatoes.com/tv/mr-robot

sistemas informáticos, suplantaciones de identidad, fraudes informáticos, estafas virtuales- bajo titulares que aluden a *hackers*:

- EE. UU. acusa a *hackers* chinos de intentar robar investigación de vacunas contra el COVID-19[377].
- Del príncipe nigeriano al *hacker* más buscado: la tenebrosa historia de Hushpuppi[378].
- Bitcoin | La billetera con 690 millones de dólares que se disputan *hackers* de todo el mundo[379].
- COVID-19 | Acusan a *hackers* chinos de robar información sobre potencial vacuna de España[380].
- Cuidado: descubren una vulnerabilidad de Windows que permite a los *hackers* tener control total de tu PC[381].
- Cuidado: *hackers* prometen ayudar a vacunarse contra el COVID-19 y roban datos personales[382].

377 "EE.UU. acusa a hackers chinos de intentar robar investigación de vacuna contra el covid-19", en *El Comercio,* Lima, 13 de mayo del 2020. https://elcomercio.pe/tecnologia/actualidad/coronavirus-covid-19-hackers-china-eeuu-acusa-a-hackers-chinos-de-intentar-robar-investigacion-de-vacuna-contra-el-covid-19-noticia/

378 "Del príncipe nigeriano al hacker más buscado: la tenebrosa historia de Hushpuppi", en *El Comercio,* Lima, 7 de julio del 2020. https://elcomercio.pe/mundo/actualidad/instagram-del-principe-nigeriano-al-hacker-mas-buscado-la-historia-de-hushpuppi-phishing-ciberdelincuentes-noticia/

379 "Bitcoin | La billetera con US$690 millones que se disputan hackers de todo el mundo", en *El Comercio,* Lima, 10 de setiembre del 2020. https://elcomercio.pe/tecnologia/tecnologia/bitcoin-la-billetera-con-us690-millones-que-se-disputan-hackers-de-todo-el-mundo-noticia/

380 "Covid 19 | Acusan a hackers chinos de robar información sobre potencial vacuna de España", en *El Comercio,* Lima, 18 setiembre del 2020. https://elcomercio.pe/tecnologia/ciencias/covid-19-acusan-a-hackers-chinos-de-robar-informacion-sobre-potencial-vacuna-en-espana-noticia/

381 "Cuidado: descubren una vulnerabilidad de Windows que permite a los hackers tener control total de tu PC", en *El Comercio,* Lima, 7 de noviembre del 2020. https://elcomercio.pe/tecnologia/ciencias/cuidado-descubren-una-vulnerabilidad-en-windows-que-permite-a-los-hackers-tener-control-total-de-tu-pc-noticia/

382 "Cuidado: hackers prometen ayudar a vacunarse contra el COVID-19 y roban datos personales", en *El Comercio,* Lima, 9 de enero del 2021. https://elcomercio.pe/tecnolo-

- Cuidado: *hackers* comienzan a estafar con la venta de vacunas falsas contra el COVID-19[383].
- Los tramposos de Call of Duty: Warzone son el nuevo objetivo de los *hackers* para distribuir *malware* de forma sencilla[384].
- *Hackers* publican datos de usuarios de más de 500 millones de cuentas de Facebook[385].
- *Hackers* rusos se infiltraron en *emails* de fiscales de EE. UU.[386]
- Poly Network | Los *hackers* que devolvieron casi la mitad de la millonaria suma que habían robado[387].
- Los *hackers* rusos y el creciente peligro de que interfieran en las elecciones alemanas[388].

---

gia/actualidad/cuidado-hackers-prometen-ayudar-a-vacunarse-contra-el-covid-19-y-roban-datos-personales-noticia/

383 "Cuidado: hackers comienzan a estafar con la venta de vacunas falsas contra el COVID-19", en *El Comercio,* Lima, 10 de marzo del 2021. https://elcomercio.pe/tecnologia/actualidad/cuidado-hackers-comienzan-a-estafar-con-la-venta-de-vacunas-falsas-contra-el-covid-19-noticia/

384 "Los tramposos de Call of Duty: Warzone son el nuevo objetivo de los hackers para distribuir malware de forma sencilla", en *El Comercio,* Lima, 2 de abril del 2021. https://elcomercio.pe/tecnologia/e-sports/los-tramposos-de-call-of-duty-warzone-son-el-nuevo-objetivo-de-los-hackers-para-distribuir-malware-de-forma-sencilla-noticia/

385 "Hackers publican datos de usuarios de más de 500 millones de cuentas de Facebook", en *El Comercio,* Lima, 5 de abril del 2021. https://elcomercio.pe/mundo/actualidad/facebook-hackers-publican-datos-de-usuarios-de-mas-de-500-millones-de-cuentas-una-red-social-business-insider-noticia/

386 "Hackers rusos se infiltraron en emails de fiscales de EE. UU.", en *El Comercio,* Lima, 31 de julio del 2021. https://elcomercio.pe/mundo/eeuu/estados-unidos-hackers-rusos-se-infiltraron-en-emails-de-fiscales-de-eeuu-rusia-solarwinds-noticia/

387 "Poly Network | Los hackers que devolvieron casi la mitad de la millonaria suma que habían robado", en *El Comercio,* Lima, 13 de agosto del 2021. https://elcomercio.pe/tecnologia/tecnologia/poly-network-los-hackers-que-devolvieron-casi-la-mitad-de-la-millonaria-suma-que-habian-robado-noticia/

388 "Los hackers rusos y el creciente peligro de que interfieran en las elecciones alemanas", en *El Comercio,* Lima, 10 de setiembre del 2021. https://elcomercio.pe/mundo/europa/rusia-los-hackers-y-el-peligro-de-que-interfieran-en-las-elecciones-de-alemania-estados-unidos-apt28-fancy-bear-noticia/

- Compras online: estos son los tipos de fraudes más utilizados por *hackers*[389].
- EE. UU. ofrece recompensa de 10 millones de dólares por los *hackers* de Darkside[390].
- El grupo de *hackers* LAPSUS$ roba credenciales de firmas de código de Nvidia para descargar *malware*[391].
- Incluso de cuentas bancarias: 6 maneras con las que *hackers* pueden robar tus contraseñas[392].
- *Hackers* dicen tener datos de 2 mil millones de usuarios de TikTok, pero plataforma niega haber tenido brecha de seguridad[393].
- Los *hackers*, el factor que pone en peligro a los sensores de los autos conectados y autónomos[394].

389 "Compras online: estos son los tipos de fraudes más utilizados por hackers", en *El Comercio,* Lima, 27 de setiembre del 2021. https://elcomercio.pe/casa-y-mas/mantenimiento/ciberdelincuencia-compras-online-estos-son-los-tipos-de-fraude-mas-utilizados-por-hackers-nndc-noticia/

390 "EE. UU. ofrece recompensa de 10 millones de dólares por los hackers de Darkside", en *El Comercio,* Lima, 4 de noviembre del 2021. https://elcomercio.pe/mundo/eeuu/estados-unidos-ofrece-recompensa-de-usd-10-millones-por-los-hackers-de-darkside-noticia/?ref=ecr

391 "El grupo de hackers LAPSUS$ roba credenciales de firmas de código de Nvidia para descargar malware", en *El Comercio,* Lima, 8 de marzo del 2022. https://elcomercio.pe/tecnologia/actualidad/nvidia-el-grupo-de-hackers-lapsus-roba-credenciales-de-firmas-de-codigo-de-nvidia-para-descargar-malware-rmmn-noticia/?ref=ecr

392 "Incluso de cuentas bancarias: 6 maneras con las que hackers pueden robar tus contraseñas", en *El Comercio,* Lima, 31 de agosto de 2022. https://elcomercio.pe/tecnologia/actualidad/ciberseguridad-6-maneras-con-las-que-hackers-pueden-robar-tus-contrasenas-incluso-de-cuentas-bancarias-espana-mexico-colombia-argentina-noticia/

393 "Hackers dicen tener datos de 2 mil millones de usuarios de TikTok, pero plataforma niega haber tenido brecha de seguridad", en *El Comercio,* Lima, 5 de setiembre de 2022. https://elcomercio.pe/tecnologia/redes-sociales/tiktok-hackers-dicen-tener-datos-de-2-mil-millones-de-usuarios-pero-plataforma-niega-haber-tenido-brecha-de-ciberseguridad-espana-mexico-colombia-noticia/

394 "Los hackers, el factor que pone en peligro a los sensores de los autos conectados y autónomos", en *El Comercio,* Lima, 13 de setiembre de 2022. https://elcomercio.pe/tecnologia/actualidad/los-hackers-el-factor-que-pone-en-peligro-a-los-sensores-de-los-autos-conectados-y-autonomos-autos-electricos-autos-autonomos-ciberseguridad-noticia/

- Uber acusa a *hackers* adolescentes Lapsus$ del ciberataque que sufrió y de la filtración de GTA 6[395].
- FBI investigará al *hacker* detrás de las filtraciones masivas de Rockstar y GTA VI[396].
- Ataque a Uber: ¿cómo operan los *hackers* como Lapsus$ que ponen en jaque a compañías internacionales?[397].
- Sitios web de aeropuertos de Estados Unidos sufren ciberataque de *hackers* prorrusos[398].
- WhatsApp: *hackers* podrían estar robando tu cuenta a través del buzón de voz[399].
- *Hacker* que robó y vendió canciones de Ed Sheeran en la *dark web* es sentenciado[400].

395 "Uber acusa a hackers adolescentes Lapsus$ del ciberataque que sufrió y de la filtración de GTA 6", en *El Comercio,* Lima, 19 de setiembre de 2022. https://elcomercio.pe/buscar/hackers/todas/descendiente/18/

396 "FBI investigará al hacker detrás de las filtraciones masivas de Rockstar y GTA VI", en *El Comercio,* Lima, 20 de setiembre de 2022. https://elcomercio.pe/tecnologia/esports/fbi-investigara-al-hacker-detras-de-las-filtraciones-masivas-de-rockstar-y-gta-vi-uber-ciberseguridad-noticia/

397 "Ataque a Uber: ¿cómo operan los hackers como Lapsus$, que ponen en jaque a compañías internacionales?", en *El Comercio,* Lima, 7 de octubre de 2022. https://elcomercio.pe/tecnologia/actualidad/ataque-a-uber-como-operan-los-hackers-como-lapsus-que-ponen-en-jaque-a-companias-internacionales-espana-estados-unidos-colombia-noticia/

398 "Sitios web de aeropuertos de Estados Unidos sufren ciberataque de hackers prorrusos", en *El Comercio,* Lima, 10 de octubre de 2022. https://elcomercio.pe/mundo/eeuu/guerra-rusia-ucrania-sitios-web-de-aeropuertos-de-estados-unidos-sufren-ciberataque-de-hackers-prorrusos-volodymyr-zelensky-vladimir-putin-rmmn-noticia/

399 "WhatsApp: hackers podrían estar robando tu cuenta a través del buzón de voz", en *El Comercio,* Lima, 17 de octubre de 2022. https://elcomercio.pe/tecnologia/actualidad/whatsapp-hackers-podrian-estar-robando-tu-cuenta-a-traves-del-buzon-de-voz-noticia/

400 "Hacker que robó y vendió canciones de Ed Sheeran en la dark web es sentenciado", en *El Comercio,* Lima, 23 de octubre de 2022. https://elcomercio.pe/tecnologia/actualidad/hacker-que-robo-y-vendio-canciones-de-ed-sheeran-en-la-dark-web-es-sentenciado-ciberseguridad-espana-mexico-usa-noticia/

- WhatsApp: qué es el "buzoneo" y cómo evitarlo para que no seas víctima de los *hackers*.[401]
- *Hackers* atacan página web de los bomberos y dificultaron recepción de emergencias[402].
- *Hackers* pro-Rusia atacan el sitio web del Parlamento Europeo[403].
- WhatsApp: *hacker* tendría en su poder los datos de casi 500 millones de usuarios[404].
- Ser *hacker* no es lo mismo que ser un cibercriminal, ¿en qué se diferencian?[405].
- *Hackers* atacan con *ransomware* hospital infantil, pero se disculpan por su falta y piden enmendarse[406].

401 "WhatsApp: qué es el 'buzoneo' y cómo evitarlo para que no seas víctima de los hackers", en *El Comercio,* Lima, 29 de octubre de 2022. https://elcomercio.pe/mag/data/whatsapp-que-es-el-buzoneo-y-como-evitarlo-para-que-no-seas-victima-de-los-hackers-tecnologia-ciberseguridad-cibercriminales-codigo-de-verificacion-nnda-nnni-noticia/

402 "Hackers atacan página web de los bomberos y dificultaron recepción de emergencias", en *El Comercio,* Lima, 8 de noviembre de 2022. https://elcomercio.pe/mag/data/whatsapp-que-es-el-buzoneo-y-como-evitarlo-para-que-no-seas-victima-de-los-hackers-tecnologia-ciberseguridad-cibercriminales-codigo-de-verificacion-nnda-nnni-noticia/

403 "Hackers pro-Rusia atacan el sitio web de Parlamento Europeo", en *El Comercio,* Lima, 23 de noviembre de 2022. https://elcomercio.pe/mundo/europa/guerra-rusia-ucrania-roberta-metsola-hackers-pro-rusia-atacan-el-sitio-web-de-parlamento-europeo-volodymyr-zelensky-vladimir-putin-rmmn-noticia/

404 "WhatsApp: hacker tendría en su poder los datos de casi 500 millones de usuarios", en *El Comercio,* Lima, 25 de noviembre de 2022. https://elcomercio.pe/tecnologia/tecnologia/whatsapp-hacker-tendria-en-su-poder-los-datos-de-casi-500-millones-de-usuarios-aplicaciones-apps-espana-mexico-usa-noticia/

405 "Ser hacker no es lo mismo que ser un cibercriminal, ¿en qué se diferencian?", en *El Comercio,* Lima, 1 de diciembre de 2022. https://elcomercio.pe/tecnologia/actualidad/cometemos-un-error-al-pensar-que-un-hacker-y-un-cibercriminal-son-lo-mismo-en-que-se-diferencian-ciberseguridad-delitos-informaticos-seguridad-espana-estados-unidos-mexico-noticia/. Después de esta publicación, los titulares comenzaron a emplear, de forma correcta, el término "ciberdelincuentes" hasta inicios de enero de 2023, en que se retomó la denominación.

406 "Hackers atacan con ransomware hospital infantil, pero se disculpan por su falta y piden enmendarse", en *El Comercio,* Lima, 5 de enero del 2023. https://elcomercio.

- Desde segundos hasta años, esto le tarda a un *hacker* descifrar tu contraseña usando la fuerza bruta[407].
- *Hacker* millonario: Capturan al autor de las estafas más conocidas del país[408].
- Un *hacker* quiso vender 9 millones de datos en Internet, pero fue detenido por las autoridades[409].
- Hackearon a los *hackers*: desmantelan Hive, importante banda de ataques de *ransomware*[410].
- Los *hackers* también pueden entrar a tu TV: estas son las formas en las que pueden hacerlo[411].
- Microsoft: falla de día cero explotada por *hackers* rusos fue corregida (atacaban correos electrónicos gubernamentales por meses)[412].

---

pe/tecnologia/actualidad/grupo-de-ransomware-se-disculpa-por-ciberataque-a-hospital-infantil-y-ofrece-herramientas-para-liberar-el-sistema-ciberseguridad-lockbit-mexico-espana-estados-unidos-noticia/

407 "Desde segundos hasta años, esto le tarda a un hacker descifrar tu contraseña usando la fuerza bruta", en *El Comercio,* Lima, 11 de enero de 2023. https://elcomercio.pe/tecnologia/actualidad/desde-segundos-hasta-anos-esto-le-tarda-a-un-hacker-descifrar-tu-contrasena-usando-la-fuerza-bruta-ciberseguridad-espana-mexico-usa-noticia/

408 "Hacker millonario: Capturan al autor de las estafas más conocidas del país", en *El Comercio,* Lima, 15 de enero de 2023. https://elcomercio.pe/videos/pais/hacker-millonario-capturan-al-autor-de-las-estafas-mas-conocidas-del-pais-nnav-video-amtv-noticia/

409 "Un hacker quiso vender 9 millones de datos en Internet, pero fue detenido por las autoridades", en *El Comercio,* Lima, 25 de enero de 2023. https://elcomercio.pe/tecnologia/actualidad/un-hacker-quiso-vender-9-millones-de-datos-en-internet-pero-fue-detenido-por-las-autoridades-ciberseguridad-privacidad-espana-mexico-estados-unidos-noticia/

410 "Hackearon a los hackers: desmantelan Hive, importante banda de ataques de ransowmare", en *El Comercio,* Lima, 26 de enero de 2023. https://elcomercio.pe/tecnologia/actualidad/hackearon-a-los-hackers-desmantelan-hive-importante-banda-de-ataques-de-ransomware-cibercriminal-estados-unidos-espana-mexico-noticia/

411 "Los hackers también pueden entrar a tu TV: estas son las formas en las que pueden hacerlo", en *El Comercio,* Lima, 20 de febrero de 2023. https://elcomercio.pe/tecnologia/actualidad/los-hackers-tambien-pueden-entrar-a-tu-tv-estas-son-las-formas-en-las-que-pueden-hacerlo-ciberseguridad-espana-mexico-usa-noticia/

412 "Microsoft: falla de día cero explotada por hackers rusos fue corregida (atacaban correos electrónicos gubernamentales por meses)", en *El Comercio,* Lima, 15 de marzo del 2023. https://elcomercio.pe/tecnologia/actualidad/microsoft-falla-de-dia-cero-ex-

- Canales de YouTube sufren ataque *hacker* masivo: usan a Elon Musk como anzuelo[413].
- *Hackers* norcoreanos usan extensiones de Chrome infectadas para robar correos Gmail a políticos[414].
- ¿Puede un auto autónomo ser controlado a distancia por un *hacker* como si fuera un arma?[415]
- El robo de US$14 millones que *hackers* llevaron a cabo en dos horas en cajeros automáticos alrededor del mundo[416].
- ¿Qué es la huella digital, por qué les interesa tanto a los *hackers* y cómo proteger la nuestra?[417]
- Miles de *hackers* realizarán un ataque masivo a los *chatbots* de IA: pondrán a prueba su seguridad[418].

---

plotada-por-hackers-rusos-fue-corregida-atacaban-correos-electronicos-gubernamentales-por-meses-ciberseguridad-espana-mexico-usa-noticia/

413 "Canales de YouTube sufren ataque hacker masivo: usan a Elon Musk como anzuelo", en *El Comercio,* Lima, 23 de marzo de 2023. https://elcomercio.pe/tecnologia/ciberseguridad/canales-de-youtube-sufren-ataque-hacker-masivo-usan-a-elon-musk-como-anzuelo-ciberseguridad-malware-espana-mexico-estados-unidos-noticia/

414 "Hackers norcoreanos usan extensiones de Chrome infectadas para robar correos Gmail a políticos", en *El Comercio,* Lima, 24 de marzo de 2023. https://elcomercio.pe/tecnologia/ciberseguridad/hackers-norcoreanos-usan-extensiones-de-chrome-infectadas-para-robar-correos-gmail-a-politicos-espana-mexico-usa-noticia/

415 "¿Puede un auto autónomo ser controlado a distancia por un hacker como si fuera un arma?", en *El Comercio,* Lima, 26 de marzo de 2023. https://elcomercio.pe/tecnologia/actualidad/puede-un-auto-autonomo-ser-controlado-a-distancia-por-un-hacker-como-si-fuera-un-arma-inteligencia-artificial-sensores-ciberseguridad-autos-electricos-automoviles-vehiculos-carros-noticia/

416 "El robo de US$14 millones que hackers llevaron a cabo en dos horas en cajeros automáticos alrededor del mundo", en *El Comercio,* Lima, 2 de abril de 2023. https://elcomercio.pe/mundo/actualidad/el-atraco-de-lazarus-el-robo-de-us14-millones-que-hackers-llevaron-a-cabo-en-dos-horas-en-cajeros-automaticos-alrededor-del-mundo-corea-del-norte-noticia/

417 "¿Qué es la huella digital, por qué les interesa tanto a los hackers y cómo proteger la nuestra?", en *El Comercio,* Lima, 19 de abril de 2023. https://elcomercio.pe/tecnologia/ciberseguridad/que-es-la-huella-digital-por-que-les-interesa-tanto-a-los-hackers-y-como-proteger-la-nuestra-ciberseguridad-cibercriminales-noticia/

418 "Miles de hackers realizarán un ataque masivo a los chatbots de IA: pondrán a prueba su seguridad", en *El Comercio,* Lima, 6 de mayo de 2023. https://elcomercio.pe/

- Un *hacker* de Destiny 2 tendrá que pagar US$12 millones por vender trampas a jugadores[419].
- *Hackers* aseguran haber robado 80 GB de datos de Reddit y exigen US$4,5 millones[420].
- Un *hacker* estaría robando criptomonedas a cientos de agentes rusos para transferirlas a Ucrania[421].
- *Hackers* filtran los datos de 2,6 millones de usuarios de Duolingo[422].
- Skype: revelan fallo de la app, *hackers* pueden conocer dirección IP con un enlace[423].
- EE. UU. dice que 60.000 *mails* del gobierno fueron pirateados por supuestos *hackers* chinos[424].

---

tecnologia/inteligencia-artificial/miles-de-hackers-realizaran-un-ataque-masivo-a-los-chatbots-de-ia-pondran-a-prueba-su-seguridad-noticia/

419 "Un hacker de Destiny 2 tendrá que pagar US$12 millones por vender trampas a jugadores", en *El Comercio,* Lima, 7 de mayo de 2023. https://elcomercio.pe/tecnologia/videojuegos/un-hacker-de-destiny-2-tendra-que-pagar-us12-millones-por-vender-trampas-a-jugadores-juicio-bungie-veterancheats-noticia/

420 "Hackers aseguran haber robado 80 GB de datos de Reddit y exigen US$4,5 millones", en *El Comercio,* Lima, 19 de junio de 2023. https://elcomercio.pe/tecnologia/ciberseguridad/hackers-aseguran-haber-robado-80-gb-de-datos-de-reddit-y-exigen-us45-millones-internet-web-phishing-ransomware-blackcat-noticia/

421 "Un hacker estaría robando criptomonedas a cientos de agentes rusos para transferirlas a Ucrania", en *El Comercio,* Lima, 20 de junio de 2023. https://elcomercio.pe/tecnologia/ciberseguridad/un-hacker-estaria-robando-criptomonedas-a-cientos-de-agentes-rusos-para-transferirlas-a-ucrania-blockchain-ciberseguridad-rusia-noticia/

422 "Hackers filtran los datos de 2,6 millones de usuarios de Duolingo", en *El Comercio,* Lima, 23 de agosto de 2023. https://elcomercio.pe/tecnologia/ciberseguridad/hackers-filtran-los-datos-de-26-millones-de-usuarios-de-duolingo-noticia/

423 "Skype: revelan fallo de la app, hackers pueden conocer dirección IP con un enlace", en *El Comercio,* Lima, 30 de agosto de 2023. https://elcomercio.pe/tecnologia/ciberseguridad/skype-revelan-fallo-de-la-app-hackers-pueden-conocer-direccion-ip-con-un-enlace-noticia/

424 "EE. UU. dice que 60.000 mails del gobierno fueron pirateados por supuestos hackers chinos", en *El Comercio,* Lima, 28 de setiembre de 2023. https://elcomercio.pe/mundo/eeuu/estados-unidos-dice-que-60000-mails-del-gobierno-fueron-pirateados-por-supuestos-hackers-chinos-video-china-microsoft-ultimas-noticia/

- *Hackers* vinculados a gobiernos de Rusia, Corea del Norte e Irán usan ChatGPT[425].
- LockBit: desmantelan al grupo de *hackers* "más dañino" del mundo tras operación internacional[426].
- ¿Cómo una megafiltración de datos ha revelado la red de *hackers* que controlaría el gobierno de China?[427]
- GooseEgg, la herramienta utilizada por *hackers* rusos para explotar vulnerabilidades de Windows[428].
- "Dirty Stream", la vulnerabilidad en populares apps Android que permite a *hackers* ejecutar código malicioso[429].
- *Hacker* expone vulnerabilidades en la NASA por segunda vez y recibe carta de agradecimiento[430].

---

425 "Hackers vinculados a gobiernos de Rusia, Corea del Norte e Irán usan ChatGPT", en *El Comercio,* Lima, 15 de febrero de 2024. https://elcomercio.pe/tecnologia/inteligencia-artificial/hackers-vinculados-a-gobiernos-de-rusia-corea-del-norte-e-iran-usan-chatgpt-openai-microsoft-estados-unidos-noticia/

426 "LockBit: desmantelan al grupo de hackers "más dañino" del mundo tras operación internacional", en *El Comercio,* Lima, 21 de febrero de 2024. https://elcomercio.pe/tecnologia/ciberseguridad/lockbit-desmantelan-al-grupo-de-hackers-mas-danino-del-mundo-tras-operacion-internacional-hackers-noticia/

427 "¿Cómo una megafiltración de datos ha revelado la red de hackers que controlaría el gobierno de China?", en *El Comercio,* Lima, 27 de febrero de 2024. https://elcomercio.pe/mundo/actualidad/china-hackers-como-una-megafiltracion-de-datos-ha-revelado-la-red-de-hackers-que-controlaria-el-gobierno-de-china-noticia/

428 "GooseEgg, la herramienta utilizada por hackers rusos para explotar vulnerabilidades de Windows", en *El Comercio,* Lima, 30 de abril de 2024. https://elcomercio.pe/tecnologia/ciberseguridad/microsoft-advierte-sobre-gooseegg-la-herramienta-utilizada-por-hackers-rusos-para-explotar-vulnerabilidades-de-windows-noticia/

429 "*Dirty Stream,* la vulnerabilidad en populares apps Android que permite a hackers ejecutar código malicioso", en *El Comercio,* Lima, 7 de mayo de 2024. https://elcomercio.pe/tecnologia/ciberseguridad/dirty-stream-la-vulnerabilidad-en-populares-apps-android-que-permite-a-hackers-ejecutar-codigo-malicioso-noticia/

430 "Hacker expone vulnerabilidades en la NASA por segunda vez y recibe carta de agradecimiento", en *El Comercio,* Lima, 27 de setiembre de 2024. https://elcomercio.pe/tecnologia/ciberseguridad/hacker-expone-vulnerabilidades-en-la-nasa-por-segunda-vez-y-recibe-carta-de-agradecimiento-noticia/

- Interbank y Plin: lo que debes hacer si eres cliente y la supuesta "negociación" con el *hacker*[431].
- ¿Puede la nueva red World reconocer humanidad y evadir a los *hackers*?[432]
- Chrome en peligro: "hackers" lograron inyectar códigos maliciosos en extensiones del popular navegador[433].

4.9.2. Breves reflexiones sobre sesgos y prejuicios

¿Por qué debe preocuparnos diferenciar los *hackers* de los ciberdelincuentes? Porque prejuzgamos negativamente un grupo social y porque los operadores jurídicos -policías, fiscales y jueces- deben evitar los sesgos tanto en la investigación criminal como en la valoración probatoria. Así, debemos evitar estigmatizar un colectivo de ciudadanos que cultivan habilidades tecnológicas que, quizás, no comprendemos totalmente.

En el *Internet User's Glossary* de 1983, la Internet Engineering Task Force definía al *hacker* como "aquella persona que disfruta tener una comprensión profunda del funcionamiento interno de un sistema, computadora o redes". Pese a ello, en el 2014, la Real Academia de la Lengua Española incluyó el término *hacker* al diccionario, pero utilizó solo una acepción: *pirata informático*. Tres años después, reconoció la segunda acepción -que subsiste hasta el día de hoy-:

431 "Interbank y Plin: lo que debes hacer si eres cliente y la supuesta "negociación" con el hacker", en *El Comercio,* Lima, 3 de noviembre de 2024. https://elcomercio.pe/lima/sucesos/a-la-filtracion-de-datos-en-interbank-se-suman-claro-topitop-y-pnp-que-hacer-tras-supuesta-fuga-de-informacion-masiva-noticia/

432 "¿Puede la nueva red World reconocer humanidad y evadir a los hackers?", en *El Comercio,* Lima, 20 de noviembre de 2024. https://elcomercio.pe/tecnologia/world-id-la-revolucion-tecnologica-que-promete-frenar-el-cibercrimen-en-america-latina-puede-la-nueva-red-world-reconocer-humanidad-y-evadir-a-los-hackers-noticia/

433 "Chrome en peligro: "hackers" lograron inyectar códigos maliciosos en extensiones del popular navegador", en *El Comercio,* Lima, 30 de diciembre de 2024. https://elcomercio.pe/tecnologia/ciberseguridad/chrome-en-peligro-hackers-lograron-inyectar-codigos-maliciosos-en-extensiones-del-popular-navegador-noticia/, publicado el 30 de diciembre de 2024.

> Persona con grandes habilidades en el manejo de computadoras que investiga un sistema informático para avisar de los fallos y desarrollar técnicas de mejora.

Llegado a este punto, debo diferenciar dos conceptos útiles en la investigación criminal, pues permitirán identificar los errores en los que podrían incurrir las víctimas y los testigos al describir un suceso delictivo: la memoria episódica y la memoria semántica. La primera está relacionada al recuerdo de sucesos y elementos en un determinado espacio temporal y espacial -por ejemplo, cuando la víctima señala que el 1 de febrero del 2022 ingresó a su cuenta de ahorros y advirtió que sustrajeron 15 mil soles, está evocando su memoria episódica-. La segunda está relacionada con el significado de la información y del conocimiento, prescindiendo del contexto espaciotemporal -por ejemplo, cuando se define el concepto *hacker*-. La profesora italiana Giuliana Mazzoni precisa que en la memoria semántica se encuentran conceptos organizados bajo la denominación de *esquemas* y *guiones* o *scripts*. Los esquemas se refieren a elementos singulares, mientras que los guiones a eventos sociales:

> Tomemos, por ejemplo, el concepto de "ladrón". Cada uno de nosotros tiene en la memoria semántica una representación esquemática del concepto "ladrón" que contiene toda una serie de elementos generales, básicos e indispensables para su comprensión. Estos elementos se refieren a aspectos como "los comportamientos y acciones que hacen de un hombre un ladrón": un ladrón no realiza un trabajo "honrado", un ladrón roba las cosas de los demás, un ladrón miente cuando se le acusa, etc. Estos elementos son esenciales en la definición de ladrón y se activan siempre que uno piensa en un ladrón. Sin embargo, además de los comportamientos necesarios que ayudan a distinguir entre quienes ladrón y quien no lo es, en el concepto de ladrón se pueden encontrar características y elementos opcionales que pueden activarse o no cuando uno piensa en el concepto abstracto de ladrón. Algunas personas insertan siempre en el esquema conceptual de ladrón otros elementos que deberían ser simplemente opcionales, por ejemplo, el concepto de "napolitano", o el de "drogadicto". Para estas personas, tales elementos forman parte integrante del concepto, están en su esquema como elementos obligatorios y, por tanto, se activan conscien-

temente, aunque también inconscientemente, en el momento en que piensan en un ladrón [...][434].

4.9.3. Los sesgos y prejuicios pueden afectar la investigación criminal y la toma de decisiones

¿Cuál es la relación de estos conceptos con los *hackers*? Bueno, los ciudadanos (víctimas o testigos) tienen una definición (esquema) o idea del *hacker*, difundida por las películas, las series, las noticias[435]: es un delincuente, es malo, actúa anónimamente, es joven, tiene conocimientos especializados, utiliza dispositivos o programas sofisticados, busca apropiarse de las cuentas, busca apropiarse del dinero de las personas, etcétera. El lector habrá caído en cuenta hacia donde se dirigen estas líneas: los prejuicios. "Una forma de prejuicio, por ejemplo, consiste en juzgar a un individuo, sin conocerlo personalmente, basándose en lo que se conoce del grupo al que pertenece o en lo que se ha oído decir. Un estereotipo es un esquema de conocimiento que afecta a un grupo de personas, es decir, un tipo especial de convicción que funciona como un filtro a través del cual se criban las informaciones que uno recibe sobre el mundo o sobre individuos pertenecientes a grupos sociales diferentes del propio"[436]. Así, la víctima o el testigo de un ciberdelito completará aquellos vacíos de su relato con los esquemas mentales que tiene y que, muchas veces, se originan en prejuicios. De esta forma, podría creer que quien accedió a su cuenta en redes sociales o a su correo electrónico o quien sustrajo dinero de su cuenta bancaria es un *hacker* -con las características que inconscientemente le atribuimos-.

De este modo, diferenciar adecuadamente los conceptos evitará adoptar decisiones erróneas durante la investigación criminal y en la decisión judicial. Si se piensa que los ciberdelitos solo pueden ser cometido por *hackers*, es decir, por personas con conocimientos altamente especializados, podríamos descartar hipótesis válidas que no calzan en estos supuestos como, por ejemplo, que el

434 Mazzoni, Giuliana. *¿Se puede creer a un testigo? El testimonio y las trampas de la memoria*. Madrid: Trotta, 2010, pp. 31 y s.

435 En esta línea, el subcapítulo denominado "Introducción: del hacker cinematográfico al cibercriminal común", en: Miró Llinares, *El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio*, cit., pp. 229-231.

436 Mazzoni, *¿Se puede creer a un testigo? El testimonio y las trampas de la memoria*, cit., pp. 45 y s.

evento delictivo haya sido realizado por alguien con escasas habilidades tecnológicas. De la misma forma, al sentenciar, el juzgador podría buscar semejanzas con algún caso que previamente haya decidido. Desarrollaré estos puntos recurriendo a los *heurísticos de representatividad* y de *accesibilidad,* así como al *sesgo de confirmación.*

Los heurísticos son atajos mentales que permiten adoptar decisiones rápidas sin tanto esfuerzo. Si bien son útiles, a veces, nos llevan a tomar decisiones erróneas. El *heurístico de representatividad* orienta a las personas a tomar decisiones a partir de lo que ya conocen y les resulta parecido a lo que tienen que decidir[437]. Sobre este punto, Cristian Contreras[438] sostiene que "llevado al terreno judicial, esto se vincula con que el juez tiende a resolver los asuntos de la misma manera en que lo ha hecho en los casos parecidos que le haya correspondido conocer previamente. Con esto simplifica enormemente su ejercicio intelectual y obtiene su decisión de forma más rápida, ya que confía en que los razonamientos que haya elaborado para casos semejantes son plenamente aplicables para el que ahora le corresponde resolver". De esta forma, si la policía o la fiscalía investigó casos de acceso ilícito que involucraron técnicas especiales o sofisticadas para su perpetración y asociaron esas ideas a la intervención de *hackers*, caerían en este heurístico si, por la similitud de la modalidad, asumen en otros casos que también deben existir *hackers* detrás de los actos ilícitos indagados.

A diferencia del heurístico de representatividad, en el que el eje central es la semejanza, en el *heurístico de accesibilidad*, es la repetición. Así, cuantas más veces se reitera un acontecimiento, más fácil será recordarlo en el futuro. Siguiendo nuevamente a Contreras, "en el plano judicial, la accesibilidad se manifiesta en que el juez tenderá a estimar más probable aquella hipótesis de los hechos que coincida con situaciones previas que pueda recordar más fácilmente, de modo que este heurístico lo llevará a pensar que en la situación actual ha sucedido lo mismo que en los ejemplos que haya podido recuperar, los que usualmente coincidirán con los casos similares que hayan acontecido en

437 Nieva Fenoll, Jordi. *La valoración de la prueba*. Madrid: Marcial Pons, 2010.

438 Contreras, Cristian. *La valoración de la prueba de interrogatorio*. Madrid: Marcial Pons, 2015, p. 112.

el último tiempo"[439]. Este es un heurístico del cual deben cuidarse las unidades especializadas en ciberdelincuencia, ya que, precisamente, investigar continuamente el mismo tipo de casos podría orientarlos a tratar nuevas denuncias como aquellos casos que han indagado previa y repetidamente.

Una de las consecuencias que se produce como efecto de este heurístico es el *sesgo de confirmación*, que se origina cuando alguien está tan convencido de un conocimiento, que, aunque *a posteriori* quede absolutamente desacreditado, tiende a continuar creyendo, pese a ello, en ese conocimiento previo. En el Recurso de Nulidad 760-2020, Lima, del 5 de abril del 2021, la Corte Suprema de Justicia advirtió que los jueces deben evitar este sesgo al juzgar y sentenciar:

> En este caso se seleccionan la información y las pruebas de acuerdo con si corroboran las preconcepciones de quien juzga, en detrimento de las hipótesis contrarias. De este modo, los jueces solo seleccionan la evidencia que confirme su hipótesis del caso y omiten aquella que sea incompatible con esta decisión. Un ejemplo de este tipo de sesgo se presenta cuando los operadores jurídicos, en el razonamiento de sus decisiones, solo citan y valoran las pruebas de la decisión que adoptaron previamente (evalúan únicamente las pruebas de cargo o únicamente las de descargo, es decir, solo valoran una parte de las pruebas actuadas) y no hacen ningún análisis de las otras pruebas (contrarias a la decisión que previamente adoptaron). Este razonamiento es claramente sesgado e irracional y, por lo tanto, carece de respaldo constitucional, pues también incurre en los vicios de motivación insuficiente y aparente.

Si quien investiga un caso tiene el prejuicio "el *hacker* es un ciberdelincuente" y considera que "los ciberdelitos son cometidos *hackers*", entonces en las indagaciones podría buscar elementos que corroboren la siguiente hipótesis: "el responsable de este ciberdelito debe ser un *hacker*". De esta forma, sobrevalorará la información que corrobore dicha perspectiva y minimizará u obviará aquella que no lo haga. Entonces, descartará inconscientemente hipótesis igualmente válidas como: pudo ser una persona de confianza que tuvo acceso a sus credenciales de autenticación por negligencia del usuario; pudo ser una

439 Contreras, *La valoración de la prueba de interrogatorio,* cit., p. 116.

persona que no tiene conocimientos avanzados, pero que adquirió los datos de acceso en el mercado negro[440]; pudo ser una persona cercana o que trabaje en la organización (*insiders*), etcétera.

Espero que estas breves reflexiones permitan alejarnos del prejuicio que cubre a la comunidad *hacker* y comprender que la dicotomía *hacker*/ciberdelincuente puede generar problemas en la investigación y en el juzgamiento.

4.10. CONCLUSIONES DEL CAPÍTULO

- Los *hackers* no son ciberdelincuentes. El tratamiento mediático y de la sociedad, en general, estigmatiza a la comunidad *hacker*, pues muchos de ellos trabajan para identificar vulnerabilidades y fortalecer la seguridad informática. Reconocer esta distinción es esencial para diseñar estrategias de ciberseguridad efectivas, mejorar las investigaciones criminales y evitar prejuicios sobre dicha comunidad.
- Algunos países han optado por modificar su Código Penal y así incluir delitos informáticos, mientras que otros han promulgado leyes especiales que los regulan. Perú, en 2013, adoptó la Ley de Delitos Informáticos, lo que permitió combatir la ciberdelincuencia de manera estructurada y con un marco jurídico robusto. A

440 Los mercados negros o ilícitos son ampliamente conocidos en la doctrina especializada: "As most users of eBay will attest, the Internet and World Wide Web provide an ideal infrastructure for the exchange of goods and services. Unfortunately, digital technology also facilities illicit online commerce. Among the first illicit online markets were those which enabled the buying and selling of stolen credit card details. The more prominent of these were ShadowCre, CarderPlanet, and DarkMarket (Glenny, 2011). The world of commerce soon expanded to include technologies for skimming and counterfeiting credit cards, malicious software such as viruses and worms (malware), and robot networks (botnets). To avoid the attention of law enforcement, many sites established elaborate processes for vetting of customers, encryption of communications, and the concealment of underground markets. These included Silk Road, which, prior to its closure in October 2013, provided an encrypted Internet forum for the purchase and sale of illegal drugs and other illicit products such as firearms, stolen credit cards, counterfeit currency, forged passport and IDs, and computer-hacking services, as well as murder for hire (Goldstein, 2013)" (Grabosky, Peter. *Cybercrime. Keynotes in Criminology and Criminal Justice Series*. New York: Oxford University Press, 2016, pp. 13 y s.).

diferencia de otras legislaciones, la nuestra resalta su objetivo principal: Prevenir y sancionar delitos que afecten datos y sistemas informáticos.

- La LDI no solo castiga los ciberdelitos, sino que también busca prevenirlos, en línea armónica con el Título Preliminar del Código Penal. La prevención eficaz de la ciberdelincuencia no es solo tarea del Estado; también involucra la educación y la concienciación ciudadana. De este modo, existen diversas iniciativas de prevención en Perú, como campañas de educación digital lideradas por el gobierno y organizaciones privadas.
- La LDI, siguiendo las recomendaciones del Convenio de Budapest, define los sistemas y datos informáticos de forma adecuada: un sistema informático es cualquier dispositivo o conjunto de dispositivos que procesa datos automáticamente. En cambio, un dato informático es toda representación de hechos, información o conceptos en un formato que pueda ser tratado electrónicamente.
- Es importante reconocer que las TIC son el medio comisivo en los delitos informáticos. Pese a que en el 2014 se suprimió la expresión *mediante las tecnologías de la información y comunicación* en la tipificación de los delitos recogidos en la LDI, su artículo 1 permite evitar confusiones sobre qué conductas pueden ser consideradas como ciberdelitos.
- La LDI no protege un solo bien jurídico, sino varios, dependiendo de su ubicación o sistematización: contra la seguridad informática (ej. acceso ilícito, sabotaje informático); contra la indemnidad y libertad sexuales (ej. *child grooming*); contra el patrimonio (ej. fraude informático); contra la fe pública (ej. suplantación de identidad).
- La ubicación de los delitos contra la interceptación ilegal de datos (art. 7 LDI) y el uso de dispositivos y mecanismos informáticos (art. 10 LDI) dificulta la identificación del bien jurídico protegido. Una eventual reforma legislativa debería incluirlos en el capítulo de "Delitos contra la seguridad informática" o de "Delitos contra los datos y sistemas informáticos" -siguiendo las recomendación del Convenio de Budapest-.

- La estructura de la LDI permite sostener que, en Perú, la seguridad informática es reconocido como un nuevo bien jurídico protegido, en atención a sus tres elementos centrales (trinomio CIA): (i) confidencialidad -protege el acceso no autorizado a los datos o sistemas informáticos-; (ii) integridad -garantizar que los datos o sistemas no sean alterados o dañados por alguien distinto a su titular o a quien este haya autorizado-; (iii) disponibilidad -asegurar que los usuarios autorizados tengan acceso cuando lo soliciten o requieran-.
- El Tribunal Constitucional ha reconocido la importancia de la seguridad en diferentes ámbitos, como la seguridad ciudadana, lo que refuerza la necesidad de considerar la seguridad informática como una prioridad estatal.
- La seguridad informática influye en decisiones legislativas trascendentales, como la tipificación de nuevos delitos, la proporcionalidad de las sanciones y la mejora de los procesos de investigación. En esta línea, la Ley de Gobierno Digital refuerza la necesidad de contar con estrategias de seguridad digital, involucrando tanto al sector público como al privado.

CAPÍTULO 5

ACCESO ILÍCITO O INTRUSISMO INFORMÁTICO



* La ilustración de la página anterior corresponde a una adaptación de *El Alquimista*, de Thomas Wijck (1640). Para su elaboración, se empleó una de las herramientas de generación de imágenes de la empresa OpenAI.

CAPÍTULO 5

ACCESO ILÍCITO O INTRUSISMO INFORMÁTICO*

Sumario: 5.1. Introducción. 5.2. Regulación en el convenio sobre la ciberdelincuencia. 5.3. Regulación en la Convención de las Naciones Unidas contra la Ciberdelincuencia. 5.4. Legislación comparada. 5.5. Legislación nacional. 5.6. El bien jurídico penalmente protegido. 5.7. El tipo penal de acceso ilícito. 5.8. Las situaciones de justificación en el delito de acceso ilícito. 5.9. Consumación. 5.10. Concursos. 5.11. Penalidad. 5.12. Circunstancias agravantes. 5.13. Propuesta normativa. 5.14. Conclusiones del capítulo.

> Todas las empresas y organizaciones son vulnerables a los ciberataques. No existe la seguridad absoluta. Constantemente somos testigos de que los agentes más sofisticados están dispuestos a dedicar importantes fondos y recursos a los ciberataques. La capacidad de recuperarse con rapidez y continuar las operaciones comerciales podría marcar la diferencia entre el éxito y el fracaso de una organización.
>
> Ann Johnson[441]

* Algunas reflexiones y comentarios de este capítulo fueron publicadas, antes de la modificación del art. 2 LDI, en Elías Puelles, Ricardo. "El delito de *hacking* o acceso ilícito a sistemas informáticos". En: *Thémis* 83, Lima: 2023.

441 Johnson, Ann. "Los profesionales de InfoSec deben aplicar la resiliencia operativa". En: Morillo, Christina (ed.). *97 cosas que todo profesional de la seguridad informática debería saber*. Madrid: Grupo Anaya, 2022, p. 24.

5.1. INTRODUCCIÓN

La investigación de los ciberdelitos no es una labor fácil, pues la volatilidad de la prueba digital exige que los operadores tengan ciertos conocimientos tecnológicos y la comunidad internacional cuente con herramientas de coope

ración eficaces[442]. Si bien los distritos fiscales de Lima Centro, La Libertad y Arequipa cuentan con fiscalías provinciales especializadas en ciberdelin-

442 No cabe duda que emplear mecanismos tradicionales como los tratados de asistencia de cooperación internacional arriesga el resultado de la investigación, pues el tiempo que demanda el procedimiento no se compara a la rapidez del ciberdelincuente al desaparecer o modificar su huella digital. Coincido con las autoras cuando sostienen lo siguiente: "De acuerdo con los enfoques tradicionales para reunir pruebas de otro país, deberían implementarse los canales diplomáticos. Sin embargo, esta parece ser una respuesta extraña cuando la información necesaria se encuentra en la computadora de los empleados de la empresa proveedora del servicio de internet, en una oficina ubicada -por ejemplo- en Estados Unidos, a solo un "clic" de distancia. Esto demuestra la necesidad de repensar los conceptos de soberanía nacional y territorialidad tradicionales. Sin embargo, debe tenerse en cuenta que los diferentes países tienen diferentes leyes con respecto al almacenamiento y protección de datos personales" (Dupuy, Daniela y Mariana Kiefer. "Datos e innovación tecnológica". En: Dupuy, Daniela [dir.]. *Cibercrimen III. Inteligencia artificial. Automatización, algoritmos y predicciones en el derecho penal y procesal penal.* Montevideo: B de F, 2022, pp. 394 y s.). En la misma línea crítica: "La consecuencia, en clave jurídica, de la transnacionalidad del delito son los problemas que surgen a partir de la investigación y, en especial, de la obtención de prueba útil y válida para el proceso. Para ello, los diversos instrumentos de asistencia internacional prevén mecanismos de colaboración. Básicamente las convenciones más modernas establecen el principio de amplitud en la prestación de colaboración y el establecimiento de una 'autoridad central' para la recepción, gestión y ejecución de los requerimientos provenientes de los otros Estados partes en el convenio que corresponda. Este mecanismo es, cuando menos, ineficiente para el desafío del delito informático, si tenemos en cuenta que estaba pensado para investigaciones o procesos judiciales puntuales y excepcionales en los que aparecía involucrado un aspecto transnacional. Pero cuando todos los delitos lo tienen -cuando en todos ellos es necesario recolectar prueba en el extranjero-, la cantidad de casos se vuelve inconmensurable y, por ende, el sistema de 'autoridad central' se hace claramente ineficiente y anacrónico" (Del Carril, Enrique H. "Desafíos del cibercrimen para el Derecho internacional". En: Dupuy, Daniela [dir.]. *Cibercrimen II. Nuevas conductas penales y contravencionales. Inteligencia artificial aplicada al derecho penal y procesal penal. Novedosos medios probatorios para recolectar evidencia digital. Cooperación internacional y victimología.* Montevideo: B de F, 2018, pp. 384 y s.).

cuencia, cuyas labores iniciaron el 15 de febrero del 2021[443] y el 7 de agosto de 2023[444], respectivamente, las investigaciones en el resto del país continúan a cargo de fiscalías penales no especializadas asistidas, de ser el caso, por la Red de fiscales en ciberdelincuencia a nivel nacional -la cual es muy importante, pero no suficiente-. A partir de un caso archivado, graficaré cuán útil es comprender los alcances del delito de acceso ilícito para planificar adecuadamente la investigación criminal[445].

[Caso 50] El 29 de octubre del 2019, una ciudadana acudió a la comisaría a presentar una denuncia verbal en los siguientes términos:

> En la ciudad de [...] siendo las 11:48:13 horas del día 29/10/2019, se presentó ante el suscrito el denunciante manifestando que el día 27/10/2019 a las 12:30:00 horas fueron víctimas del jaqueado de sus correos, por parte de personas desconocidas, quienes empleando medidas de engaño solicitaban las cuentas de correo, número de celulares y asimismo que había un trabajo de campaña de enviar fotos de chicas desnudas para campaña de cáncer de seno, a lo cual pagarían la suma de 500 soles. Cabe mencionar que la agraviada fue jaqueada de su correo el 28OCT19, a horas 21:00, desconociendo quiénes serían autores del hecho. Asimismo, refieren que dicha denuncia obre como constancia, lo que denuncia ante la Policía Nacional del Perú para los fines consiguientes, firmando la presente acta en presencia del instructor [sic].

Al día siguiente, la comisaría remitió el acta de denuncia verbal al Ministerio Público. Dos semanas después, el 18 de noviembre del 2019, sin realizar actos de investigación, se archivó el caso, argumentando que no se identificó al posible autor del evento criminal:

---

443 Ministerio Público del Perú. *Resolución de la Fiscalía de la Nación N.º 1503-2020-MP-FN, Crean la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público con competencia nacional y designan y nombran Fiscales en el Distrito Fiscal de Lima*. Lima: 30 de diciembre del 2020.

444 Ministerio Público del Perú. *Resolución de la Junta de Fiscales Supremos N.º 061-2023-MP-FN-JFS*. Lima: 12 de agosto del 2023.

445 Este relato pertenece a una denuncia real, sin embargo, eliminé todo dato personal que permita identificar a la víctima o la unidad policial/fiscal que estuvo a cargo.

> Ahora, respecto a la individualización de los imputados se tiene únicamente el dicho de las denunciantes, quienes refieren que se trató de sujetos desconocidos; no contando con otros elementos que permitan dicha individualización y posterior identificación, por lo que, en este estado no resulta posible sostener la tesis incriminatoria contra una persona determinada; lo que resulta necesario, pues todo proceso penal, para poder llevarse a cabo, requiere de un imputado debidamente determinado, plenamente individualizado, como presunto autor de un hecho ilícito [...]. De lo mencionado hasta el momento, se tiene que la acción penal no ha prescrito y existen indicios de la existencia del delito; pero no se ha identificado a su o sus autores; por lo que corresponde aplicar lo establecido en el numeral 3 del artículo 334 del Código Procesal Penal, solicitando a la Policía Nacional del Perú que, a través de sus unidades especializadas, continúe con los actos de investigación tendientes a la consecución de dicho fin. Precisándose a su vez, que el presente caso podrá ser reexaminado en el supuesto que se descubran con posterioridad nuevos elementos de convicción [...] [sic].
>
> **Decisión Fiscal** [...] 1. Que, no procede formalizar ni continuar con la investigación preparatoria contra los que resulten responsables por la presunta comisión de delito informático en agravio de [...], ordenándose el archivo de lo actuado.
>
> 2. Notificar con la presente disposición a la DIVINCRI PNP a efectos, por intermedio de sus unidades especializadas en esta clase de ilícitos, realice los actos de investigación tendientes a la ubicación del o los responsables del hecho denunciado; debiendo informar a este despacho si los resultados arribados son positivos.

Esta decisión fue notificada a la denunciante, quien no interpuso recurso de elevación de actuados -en palabras sencillas, no *cuestionó* la decisión-. De esta forma, en vez de abrir la investigación preliminar, la fiscalía archivó el caso, ordenando que la carpeta sea remitida a la policía. A continuación, analizaré algunos problemas en la recepción de la denuncia verbal y en el archivo del caso:

- En primer lugar, la redacción del acta no permite conocer si nos encontramos frente a una, dos o más víctimas. Este punto es relevante para identificar el objetivo del ciberdelincuente: ¿una persona específica, un grupo que comparte algún vínculo o simplemente víctimas al azar?

- En segundo lugar, el acta no recoge información adicional sobre la hora del ataque: ¿cómo se sabe que fue a las 12:30:00?, ¿acaso se recibió una alerta sobre la vulneración del sistema informático? Hubiese sido importante profundizar este punto y, así, conocer los detalles del acceso ilícito.
- En tercer lugar, no se precisan las cuentas de correo electrónico cuyas medidas de seguridad fueron vulneradas. Conocer esta información permitiría saber si nos encontramos frente a una posible brecha de seguridad o, quizás, ante un *malware* que permite capturar contraseñas o ejecutar otra acción ilícita.
- En cuarto lugar, no se solicitó información sobre las medidas de seguridad que protegen los correos electrónicos vulnerados. Así, el agente policial que recibió la denuncia debió resolver, entre otras, las siguientes interrogantes: ¿cuán robustas son la contraseñas?, ¿cuenta con autentificación en dos pasos?, ¿ha compartido su contraseña con alguna persona cercana?, ¿escribe su contraseña en algún lugar al cual pueden acceder otras personas? Como veremos en este capítulo, el artículo 2 LDI, recoge la vulneración de las *medidas de seguridad* como una modalidad agravada. Por esta razón, es importante no solo conocer si contaba con dichas medidas, sino, también, requerir más información para trazar eventuales líneas de investigación que permitiese responder si fueron vulneradas de manera presencial o remota.
- En quinto lugar, la víctima precisa que no conoce la identidad del ciberdelincuente o de quienes se encuentran detrás de este ilícito accionar -como pasa frecuentemente en este tipo de casos-. Sin embargo, esta no es una razón válida para que se archive la denuncia sin realizarse un solo acto de indagación. Así, para iniciar diligencias preliminares no se requiere identificar al responsable. El Ministerio Público pudo trazar un plan de investigación orientado al aseguramiento de las pruebas y la identificación del ciberdelincuente, pero no lo hizo. Ya sea que la víctima dejó consentir el pronunciamiento por desinterés o por ausencia de asesoría adecuada, lo cierto es que no se logró conocer quién o quiénes estuvieron detrás del ataque.

Debo precisar que el caso analizado no tiene por finalidad cuestionar la labor de la Policía o el Ministerio Público, pues existen muchos operadores comprometidos en la lucha frontal contra la ciberdelincuencia, sino únicamente ejemplificar lo que sucede cuando un caso no es atendido de forma diligente.

[Caso 51] Lamentablemente, suele suceder que algunos casos emblemáticos generan cambios estructurales y normativos en la sociedad. Esto fue lo que sucedió en Brasil. En el 2012, la cantante y actriz Carolina Dieckmann recibió y abrió un correo electrónico malicioso. El atacante accedió a su buzón y encontró una treintena de fotografías de contenido erótico, las cuales descargó y utilizó para solicitar dinero, a cambio de no divulgarlas. Inicialmente, pensó que el servicio técnico que reparó su computadora meses atrás pudo acceder a las fotografías, pero dicha hipótesis se descartó al encontrarse a los verdaderos responsables: jóvenes de poco más de veinte años que dirigieron el ataque. Rodrigo Valle, inspector del Grupo de Operaciones de la Policía brasileña brindó una entrevista en la que detalló la forma de operar:

> Fue por el uso de un *software* malicioso enviado a su cuenta de correo electrónico, que llamamos *spam,* y la víctima fatalmente hizo clic en este *spam*, abrió este *spam* en su computadora o portátil o en su propio PC y probablemente dejó que este archivo fuera reenviado, respondido al autor[446] [Traducción propia].

El caso de la actriz generó tanta preocupación, ya que Brasil no contaba con legislación especializada en la materia, que el 30 de noviembre del 2012 se promulgó la Ley 12737, conocida como ley Carolina Dieckmann. De este modo, los delitos informáticos fueron incorporados al ordenamiento penal de dicho país[447].

446 "Polícia encontra hackers que roubaram fotos de Carolina Dieckmann", en *Fantástico*, Sao Paulo, 13 de mayo de 2012 [actualizado el 11 de diciembre de 2012]. https://g1.globo.com/fantastico/noticia/2012/05/policia-encontra-hackers-que-roubaram-fotos-de-carolina-dieckmann.html

447 Messagi, Mário. *Lei Carolina Dieckmann é sancionada; saiba o que muda na legislação para a internet*, publicado el 5 de diciembre de 2012. https://jornalcomunicacao.ufpr.br/lei-carolina-dieckmann-e-sancionada-pela-presidente-dilma-saiba-o-que-muda-na-legislacao-da-internet/

En las líneas siguientes analizaré cómo se encuentra regulado el delito de acceso ilícito en el Convenio sobre la Ciberdelincuencia, al cual Perú se adhirió en el 2019, y comentaré brevemente los párrafos 44 a 50 de su Informe Explicativo, pues permiten interpretar sus alcances. Luego, analizaré su tipificación en la Convención de las Naciones Unidas contra la Ciberdelincuencia. Acto seguido, citaré legislación comparada de los países de la región que también se han adherido al Convenio con la finalidad de conocer las modalidades recogidas y su afinidad con la legislación peruana. Finalmente, realizaré un breve recuento sobre la evolución del delito de acceso ilícito desde su incorporación al Código Penal, en el 2000, hasta su actual regulación en la LDI.

5.2. REGULACIÓN EN EL CONVENIO SOBRE LA CIBERDELINCUENCIA

Como he señalado previamente, bajo el título *Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos*, el Convenio recoge el acceso ilícito (art. 2 Conv.), la interceptación ilícita (art. 3 Conv.), los ataques a la integridad de los datos (art. 4 Conv.), los ataques a la integridad del sistema (art. 5 Conv.) y el abuso de los dispositivos (art. 6 Conv.).

El delito de acceso ilícito se encuentra previsto en los siguientes términos:

> **Art. 2.- Acceso ilícito**
>
> Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno el acceso deliberado e ilegítimo a todo o parte de un sistema informático. Las Partes podrán exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos u otra intención delictiva, o en relación con un sistema informático conectado a otro sistema informático.

Esta fórmula legislativa puede graficarse de la siguiente forma:

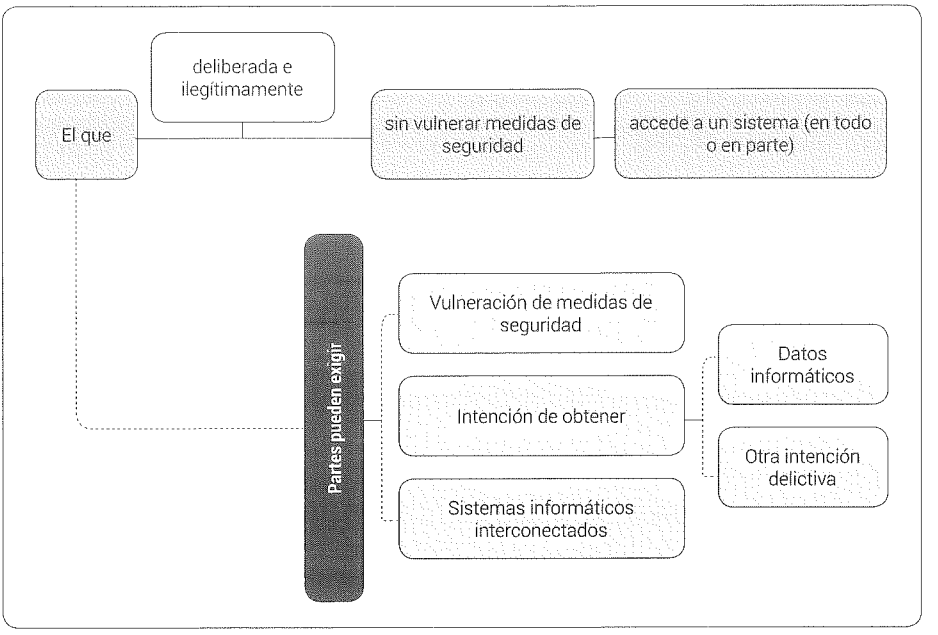


Diagrama 6. Estructura del delito de acceso ilícito, propuesto en el Convenio de Budapest. Elaboración propia.

El artículo 40 de la Convención prevé que los Estados podrán declarar, en el momento de la firma o del depósito del instrumento de ratificación, aceptación, aprobación o adhesión, que se acogen a la facultad de exigir, llegado el caso, uno o más elementos complementarios. Es en uso de esta facultad que Perú realizó la siguiente declaración:

> **Texto de la declaración**
>
> De conformidad con lo dispuesto en el artículo 2 del Convenio sobre la Ciberdelincuencia, la República del Perú declara que su legislación exige que el delito de acceso ilícito se cometa infringiendo medidas de seguridad.

Cada artículo del Convenio ha sido desarrollado en el Informe Explicativo. En el caso del delito de acceso ilícito, los párrafos 44 a 50 recogen algunas ideas muy importantes que resumo a continuación y que, en algunos casos, comentaré brevemente:

- El párrafo 44 indica que el acceso ilícito es un *delito básico* que amenaza peligrosamente o ataca la seguridad informática, compuesta por la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos. Además, se distinguen tres modalidades que suelen equipararse: (i) mera intrusión no autorizada, piratería o *hacking*; (ii) el sabotaje o *cracking*; y (iii) la intrusión en el ordenador o *computer trespass*. Así, se precisa que este delito "puede constituir un impedimento para los usuarios legítimos de los datos y sistemas y puede causar alteración o destrucción [...]", sin embargo, he de indicar que no es condición necesaria o el paso previo indispensable para la comisión de otros ciberdelitos[448].
- El párrafo siguiente resalta la importancia de las medidas de seguridad para la prevención del acceso ilícito. Sobre este punto, es importante recordar que nuestro país exige la vulneración de las medidas en referencia para su configuración típica.
- En el párrafo 46, se define el término *acceso* como "la entrada a un sistema informático o a alguna parte del mismo (*hardware*, componentes, datos almacenados del sistema instalado, directorios, datos relativos al tráfico y datos relacionados con los contenidos)". Además, se precisa que esta definición incluye "el ingreso a otro sistema informático, al que esté conectado a través de redes de telecomunicaciones públicas, o a un sistema informático que esté conectado a la misma red, como una LAN (red de área local) o una Intranet (red interna) que opere en el seno de una organización".
- El párrafo siguiente precisa que la conducta debe ser cometida de manera ilegítima y que este no es el caso del acceso autorizado para realizar una verificación o protección del sistema informático, ni tampoco al ingresar a sistemas que permiten el acceso libre

448 El profesor argentino Aboso anota que el Convenio de Budapest no establece condiciones objetivas ni subjetivas para la tipificación del delito de acceso ilícito, es decir, no requiere que el ingreso no autorizado haya vulnerado medidas de seguridad ni demanda una especial intención especial del autor (Aboso, Gustavo Eduardo. *Derecho penal cibernético: La cibercriminalidad y el derecho penal en la moderna sociedad de la información y la tecnología de la comunicación*. Montevideo: B de F, 2018, p. 177).

y abierto al público. Sobre este punto, he de indicar que la LDI fue modificada para incluir expresamente los términos *deliberada* e *ilegítimamente*, pese a que no era necesario -como expliqué en el capítulo anterior-.

- El párrafo subsiguiente nos recuerda que el mantenimiento de un sitio web o la aplicación de herramientas estándar provistas en los protocolos y programas de comunicación no es *per se* ilegítima. Grafica este punto con el uso de *cookies*, ya que pueden ser rechazadas o eliminadas por el usuario que accede a las páginas.
- El párrafo 49 resalta la controversia que existe sobre la tipificación del mero intrusismo, ya que la legislación de algunos países no sanciona el acceso que no crea peligro alguno en el usuario o que ayuda a detectar *agujeros* o puntos débiles de los sistemas de seguridad. No es el caso peruano, pues, como veremos más adelante, sí sanciona esta modalidad.
- Finalmente, el párrafo 50 remarca que los Estados tienen la posibilidad de tipificar el acceso ilícito, exigiendo (i) la vulneración de las medidas de seguridad, (ii) con una intención delictiva o (iii) cuando se afecten sistemas informáticos interconectados. Es importante recordar que, si bien Perú incorporó la vulneración de medidas de seguridad como elemento adicional del tipo penal en la LDI original, se eliminó este requisito en la modificación de diciembre del 2023.

5.3. REGULACIÓN EN LA CONVENCIÓN DE LAS NACIONES UNIDAS CONTRA LA CIBERDELINCUENCIA

El artículo 7 de la Convención recoge el delito de acceso ilícito en los siguientes términos:

> **Art. 7.- Acceso ilícito**
>
> 1. Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para tipificar como delito en su derecho interno el acceso deliberado y sin derecho a la totalidad o una parte de un sistema de tecnología de la información y las comunicaciones.

2. Los Estados partes podrán exigir como requisito que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos electrónicos o con otra intención deshonesta o delictiva o en relación con un sistema de tecnología de la información y las comunicaciones que esté conectado a otro sistema de tecnología de la información y las comunicaciones.

La fórmula es similar a la del Convenio de Budapest; sin embargo, introduce una ligera modificación. En este caso, no se hace alusión a sistemas informáticos, sino a sistemas de tecnología de la información y las comunicaciones. En todo lo demás, guarda estrecha relación con el Convenio previamente analizado.

5.4. LEGISLACIÓN COMPARADA

Conocer la regulación del delito de acceso ilícito en la legislación del resto de países latinoamericanos que se adhirieron al Convenio de Budapest[449], así como en España por su gran influencia en la materia, permitirá comparar su marco punitivo y conocer modalidades no previstas en Perú.

País	Legislación	Tipo penal
Países latinoamericanos que se adhirieron al Convenio de Budapest		
Ecuador	**Código Orgánico Integral Penal**	**Sección Tercera. Delitos contra la seguridad de los activos de los sistemas de la información y comunicación** **Art. 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones** 1. La persona que sin autorización acceda a todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho sobre dicho sistema, será sancionada con la pena privativa de la libertad de tres a cinco años. 2. Si la persona que accede al sistema lo hace para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar el tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a las o los proveedores de servicios legítimos, será sancionada con pena privativa de libertad de tres a cinco años.
Brasil	**Código Penal**	**Seção IV. Dos Crimes contra a inviolabilidade dos segredos** **Art. 154-A.- Invasão de dispositivo informático** 1. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita: Pena-reclusão, de 1 (um) a 4 (quatro) anos, e multa.

449 El orden de los países no es aleatorio, sino que inicia con Ecuador -cuya adhesión es la más reciente- y continúa hasta República Dominicana -la más antigua de la región-.

País	Legislación	Tipo penal
Colombia	Código Penal	**Título VII-A. De delitos contra el patrimonio cultural sumergido** **Art. 269 A.- Acceso abusivo a un sistema informático** El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo.
Paraguay	Código Penal	**Capítulo VII. Hechos punibles contra el ámbito de vida y la intimidad de la persona** **Art. 146 B.- Acceso indebido a datos** 1. El que sin autorización y violando sistemas de seguridad obtuviere para sí o para terceros, el acceso a datos no destinados a él y especialmente protegidos contra el acceso no autorizado, será castigado con pena privativa de libertad de hasta tres años o multa. 2. Como datos en sentido del inciso 1º, se entenderán solo aquellos, que se almacenan o transmiten electrónicamente, magnéticamente o de otra manera no inmediatamente visible. **Art. 174 B.- Acceso indebido a sistemas** 1. El que accediere a un sistema informático o a sus componentes, utilizando su identidad o una ajena; o excediendo una autorización, será castigado con pena privativa de libertad de hasta tres años o multa. 2. Se entenderá como sistema informático a todo dispositivo aislado o al conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus componentes, sea el tratamiento de datos por medio de un programa informático.
Argentina	Código Penal	**Capítulo III. Violación de los secretos y de la privacidad** **Art. 153 bis.-** Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido. La pena será de un (1) mes a un (1) año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros.
Costa Rica	Código Penal	**Sección I. Violación de secretos. Violación de correspondencia** **Art. 196.- Violación de correspondencia o comunicaciones** Será reprimido con pena de prisión de uno a tres años a quien, con peligro o daño para la intimidad o privacidad de otro, y sin su autorización, se apodere, acceda, [...] abra, [...] documentación o comunicaciones dirigidas a otra persona. [...] La misma pena se impondrá a quien promueva, incite, instigue, prometa o pague un beneficio patrimonial a un tercero para que ejecute las conductas descritas en los dos párrafos anteriores. La pena será de dos a cuatro años de prisión si las conductas descritas en el primer párrafo de este artículo son realizadas por: a) Las personas encargadas de la recolección, entrega o salvaguarda de los documentos o comunicaciones. b) Las personas encargadas de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tengan acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos. **Artículo 196 bis.- Violación de datos personales** Será sancionado con pena de prisión de uno a tres años quien en beneficio propio o de un tercero, con peligro o daño para la intimidad o privacidad y sin la autorización del titular de los datos, se apodere, [....] acceda, [...] a las imágenes o datos de una persona física o jurídica almacenados en sistemas o redes informáticas o telemáticas, o en contenedores electrónicos, ópticos o magnéticos. La pena será de dos a cuatro años de prisión cuando las conductas descritas en esta norma: a) Sean realizadas por personas encargadas de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tengan acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos. b) La información vulnerada corresponda a un menor de edad o incapaz. c) Las conductas afecten datos que revelen la ideología, la religión, las creencias, la salud, el origen racial, la preferencia o la vida sexual de una persona.

País	Legislación	Tipo penal
Chile	Ley N.° 21459	**Título I. De los delitos informáticos y sus sanciones** **Art. 2.- Acceso ilícito** El que, sin autorización o excediendo la autorización que posea y superando barreras técnicas o medidas tecnológicas de seguridad, acceda a un sistema informático será castigado con la pena de presidio menor en su grado mínimo o multa de once a veinte unidades tributarias mensuales. Si el acceso fuere realizado con el ánimo de apoderarse o usar la información contenida en el sistema informático, se aplicará la pena de presidio menor en sus grados mínimo a medio. Igual pena se aplicará a quien divulgue la información a la cual se accedió de manera ilícita, si no fuese obtenida por éste. En caso de ser una misma persona la que hubiere obtenido y divulgado la información, se aplicará la pena de presidio menor en sus grados medio a máximo. No será objeto de sanción penal por haber incurrido en los hechos tipificados en el inciso primero, el que habiendo accedido a un sistema informático cuyo responsable tenga domicilio en Chile, lo hiciera cumpliendo con las siguientes condiciones: 1. Que se encuentre inscrito en el registro que al efecto lleve la Agencia Nacional de Ciberseguridad. 2. Que el acceso se haya realizado habiendo informado previamente de ello a la Agencia. 3. Que el acceso y las vulnerabilidades de seguridad detectadas hayan sido reportadas al responsable del sistema informático y a la Agencia, tan pronto se hubiere realizado. 4. Que el acceso no haya sido realizado con el ánimo de apoderarse o de usar la información contenida en el sistema informático, ni con intención fraudulenta. Tampoco podrá haber actuado más allá de lo que era necesario para comprobar la existencia de una vulnerabilidad, ni habrá utilizado métodos que pudieran conducir a denegación de servicio, a pruebas físicas, utilización de código malicioso, ingeniería social y alteración, eliminación, exfiltración o destrucción de datos. 5. Que no haya divulgado públicamente la información relativa a la potencial vulnerabilidad. 6. Que se trate de un acceso a un sistema informático de los organismos de la Administración del Estado. En el resto de los casos, requerirá del consentimiento del responsable del sistema informático. 7. Que haya dado cumplimiento a las demás condiciones sobre comunicación responsable de vulnerabilidades que al efecto hubiere dictado la Agencia.
Panamá	Código Penal	**Capítulo I. Delitos contra la seguridad informática** **Art. 289.-** Quien indebidamente ingrese o utilice una base de datos, red o sistema informático será sancionado con dos a cuatro años de prisión.
República Dominicana	Ley N.° 53-07	**Capítulo I. Crímenes y delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos** **Art. 6.- Acceso ilícito.-** El hecho de acceder a un sistema electrónico, informático, telemático o de telecomunicaciones, o a sus componentes, utilizando o no una identidad ajena, o excediendo una autorización, se sancionará con las penas de tres meses a un año de prisión y multa desde una vez a doscientas veces el salario mínimo.
Otras referencias		
España	Código Penal	**Capítulo I. Del descubrimiento y revelación de secretos** **Art. 197 *bis*.-** 1. El que, por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años.

Cuadro 15. Legislación comparada respecto al delito de acceso ilícito. Elaboración propia.

Al revisar la legislación, se advierte que ningún otro estado incluye los elementos *deliberada* e *ilegítimamente* como parte de la construcción del tipo

penal de acceso ilícito. ¿La ausencia de dichos elementos impidió su adhesión al Convenio de Budapest? No, pues son elementos innecesarios y que, más bien, dificultan el juicio de subsunción.

Además, podemos advertir que la ubicación del delito de acceso ilícito es dispar en la legislación comparada -lo que impactará en la delimitación del bien jurídico protegido y las conductas que pueden constituir este ilícito-. De este modo, por ejemplo, (1) Argentina, Brasil, Costa Rica y España lo ubican en el capítulo de delitos contra la revelación de secretos; (2) Paraguay lo sitúa junto a los delitos contra la intimidad o privacidad; (3) Ecuador, Chile, Panamá y República Dominicana lo ubican en el capítulo que sanciona los delitos informáticos, contra la seguridad informática o contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos; y, finalmente, (4) Colombia, como parte de los delitos contra un tipo especial de patrimonio.

En cuanto a la denominación del objeto vulnerado, es variado, según la legislación analizada. De este modo, se emplean diferentes denominaciones: *sistema informático*, *sistema electrónico*, *sistema telemático*, *sistema de telecomunicaciones*, *base de datos*, *red*, *contenedores electrónicos*, *contenedores magnéticos*, *contenedores ópticos*. Sería importante que las regulaciones latinoamericanas uniformicen los términos empleados al amparo del Convenio de Budapest o la Convención de las Naciones Unidas en aras de evitar ambigüedades, garantizando así, el principio de legalidad (*lex certa*).

No todos los países exigen el quebrantamiento de medidas de seguridad. Entre los que sí lo hacen, se encuentran: Chile (barreras técnicas o medidas tecnológicas de seguridad), España (medidas de seguridad) y Paraguay (sistemas de seguridad).

Si bien todos los países sancionan el acceso ilícito, se aprecia que Ecuador, España y Colombia tipifican la ocupación indebida, es decir, mantenerse en el sistema, pese a que su titular exige la salida. De otro lado, Argentina, Chile, Colombia, Paraguay y República Dominicana castigan a quien legítimamente accede al sistema, pero que indebidamente excede la autorización brindada.

Finalmente, para la configuración de una forma agravada, Brasil, Chile y Ecuador exigen un elemento de tendencia interna trascendente, es decir, el ciberdelincuente deberá acceder, persiguiendo una finalidad ilegal adicional. En el resto de legislaciones estudiadas, este elemento no se encuentra presente.

5.5. LEGISLACIÓN NACIONAL

A continuación, analizaré el delito de acceso ilícito en la legislación penal peruana. Para ello, iniciaré explicando su incorporación al CP y, luego, el camino que siguió para su inclusión y regulación actual en la LDI.

5.5.1. Antecedentes normativos

Ocho años después de la promulgación del CP de 1991, se presentaron tres proyectos de ley que originaron la incorporación del *Capítulo X. Delitos Informáticos* al ordenamiento[450], pero solo dos de ellos incidieron en la seguridad informática:

- **Proyecto de Ley N.º 5071/99-CR**, presentado el 18 de agosto de 1999 por el congresista Jorge Muñiz Ziches. Esta iniciativa recogió la redacción más cercana del tipo penal bajo estudio[451].
- **Proyecto de Ley N.º 5132/99-CR**, presentado el 31 de agosto de 1999 por la congresista Susana Díaz Díaz. Cobijó una modalidad del delito de acceso ilícito que no prosperaría[452].

Cuatro meses después, ambos proyectos obtuvieron un dictamen unánime favorable por parte de la Comisión de Reforma de Códigos del Congreso de la República, debiendo resaltar que no hubo debate sobre el bien jurídico tutelado, ya que se aceptó, sin dudas o cuestionamientos, que se trataba del patrimonio. No obstante, en atención a las observaciones remitidas por el Poder Ejecutivo, se tuvo que aprobar un texto sustitutorio. Así, finalmente, una modalidad del delito de acceso ilícito fue recogida en el artículo 207-A CP:

---

450 Sobre este punto, ver el capítulo tres de esta publicación.

451 **Proyecto de Ley N.º 5071/99-CR, art 208-A.-** El que indebidamente utilice o ingrese a una base de datos, sistema o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio con el fin de defraudar, obtener dinero, bienes o información será reprimido con pena privativa de libertad no mayor de dos años, o con prestación de servicios comunitario de [cincuenta y dos] a ciento cuatro jornadas.

452 **Proyecto de Ley N.º 5132/99-CR, art. 2.-** El que, con ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, lo interfiera o acceda a él, será reprimido con pena privativa de libertad no mayor de tres años.

Art. 207-A CP.- Delito informático

El que utiliza o ingresa indebidamente a una base de datos, sistema o red de computadoras o cualquier parte de la misma, para diseñar, ejecutar o alterar un esquema u otro similar, o para interferir, interceptar, acceder o copiar información en tránsito o contenida en una base de datos, será reprimido con pena privativa de libertad no mayor de dos años o con prestación de servicios comunitarios de [cincuenta y dos] a ciento cuatro jornadas.

Si el agente actuó con el fin de obtener un beneficio económico, será reprimido con pena privativa de libertad no mayor de tres años o con prestación de servicios comunitarios no menor de ciento cuatro jornadas.

El artículo 207-A CP, incorporado el 17 de julio del 2000, sancionaba el acceso indebido sin exigir la ruptura de medidas de seguridad, pero sí requería una finalidad delictiva posterior para su configuración, erigiéndose como un delito de tendencia interna trascendente. Por su ubicación sistemática, cierto sector consideraba que se protegía el patrimonio; no obstante, voces críticas opinaban que se sancionaban los ataques contra la seguridad informática[453].

Esta norma fue derogada el 22 de octubre del 2013 con la promulgación de la LDI[454].

---

453 "No obstante, consideramos que el bien jurídico protegido en el tipo penal del artículo 207-A es la seguridad informática, ya que la conducta descrita se refiere a la utilización o ingreso indebido a una base de datos, sistema o red de computadoras, lo cual está en relación a la afectación de la seguridad informática y no del patrimonio o la intimidad, en cuanto se lesiona una de sus manifestaciones como es el acceso o su utilización indebida" (Durand Valladares, Raúl. "Los delitos informáticos en el Código Penal peruano". En: *Revista Peruana de Ciencias Penales* 11. Lima: 2002, p. 309).

454 "En el artículo 207-A si bien se sanciona la utilización o ingreso indebido a una base de datos o sistemas informáticos, con la finalidad de diseñar, ejecutar, interferir, interceptar, existirán problemas para distinguir el denominado *hacking blanco*, máxime cuando el propio legislador concibe como finalidad del ingreso el acceso, luego no puede darse una conducta de ingresar para acceder. No obstante, debemos señalar que, en cuanto al aspecto subjetivo, el primer párrafo del artículo 207-A exige las finalidades antes descritas como elementos subjetivos de intención trascendente, no siendo necesario su realización material" (Durand Valladares, "Los delitos informáticos en el Código Penal peruano", cit., p. 311).

5.5.2. Génesis legislativa

A mediados del 2011, se recibió la primera propuesta legislativa que generaría cambios significativos en la lucha peruana contra ciberdelincuencia. Si bien fueron ocho proyectos que desembocaron en la promulgación de la LDI, solo dos se refirieron al delito de acceso ilícito:

- **Proyecto de Ley N.° 34/2011-CR**, presentado el 11 de agosto de 2011 por el congresista Juan Carlos Eguren Neuenschwander. Esta iniciativa propuso un cuerpo normativo independiente por el nivel de especialidad que tiene la informática y la posibilidad de incluir disposiciones procesales para facilitar su investigación.

  Respecto al delito bajo análisis: (i) No exigía la vulneración de medidas de seguridad, (ii) incluía la interceptación e interferencia de sistemas informáticos como conductas prohibidas, (iii) no recogía el abuso de confianza como modalidad de acceso indebido[455].

- **Proyecto de Ley N.° 2520/2012-PE**, presentado el 26 de julio de 2013 por el presidente de la República Ollanta Humala Tasso. Esta iniciativa recogió la redacción exacta del tipo penal que originalmente fue incluido en la LDI[456].

5.5.3. Evolución legislativa

Como he señalado anteriormente, la LDI adoptó los nueve capítulos sugeridos en el proyecto de Ley N.° 34/2011-CR, propuesta que, bajo el nombre de *Delitos contra los Sistemas de Información y las Tecnologías de la Comunicación*, recomendó la tipificación de cinco delitos: (i) intrusismo in-

455 **Proyecto de Ley N.° 34/2011-CR, art 3.-** ***Intrusismo Informático.*** El que sin la debida autorización acceda, intercepte o interfiera un sistema de información o una tecnología de información, será reprimido con una pena privativa de libertad no menor de uno ni mayor de tres años.

456 **Proyecto de Ley N.° 2520/2012-PE, art 208-A.-** ***Acceso ilícito.*** El que accede sin autorización a todo o en parte de un sistema informático siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días multa.
Será reprimido con la misma pena el que accede a un sistema informático excediendo lo autorizado.

formático, (ii) sabotaje informático, (iii) intrusismo o sabotaje de sistemas o tecnologías de información con medidas de seguridad o información especial, (iv) prestación de equipos y servicios con fines de intrusismo y/o sabotaje y (v) espionaje informático. Sin embargo, fue el proyecto de Ley N.º 2520/2012-PE el que terminó por imponer su propuesta de redacción. Este último proyecto recomendó incorporar el Título V-A al CP o *Atentado contra los datos y sistemas informáticos*, el cual tendría cuatro capítulos, de los cuales me interesa resaltar el primero, pues recoge el delito de acceso ilícito.

El capítulo II de la LDI se denomina *Delitos contra datos y sistemas informáticos* y agrupa el delito de acceso ilícito (art. 2 LDI), el atentado contra la integridad de datos informáticos (art. 3 LDI) y el atentado contra la integridad de sistemas informáticos (art. 4 LDI). Un lector acucioso podría preguntar: ¿se atentan contra los datos informáticos al acceder sin autorización a un sistema? Como he señalado líneas atrás, sostengo que no; sin embargo, ¿por qué fueron agrupados de esta manera? Porque se emplea el título propuesto en el proyecto de Ley N.º 2520/2012-PE que, a su vez, se inspira en el Convenio de Budapest, pero que recortó la expresión completa -la que le hubiera dado sentido-: *Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos.*

Un mes después de la promulgación de la LDI, se recibieron dos propuestas legislativas que modificaron diversos delitos -entre ellos, el acceso ilícito-, a saber:

a. **Proyecto de Ley N.º 2991/2013-CR**, presentado el 25 de noviembre de 2013 por el congresista Juan Carlos Eguren Neuenschwander. Esta iniciativa propuso incorporar las expresiones *deliberada* e *ilegítima*, ya que, según su autor, la LDI "no cumple con algunos de los estándares previstos en el Convenio sobre la Cibercriminalidad (Convenio de Budapest) en el sentido de no haber incorporado en la redacción típica de los delitos [...] la calidad de deliberada e ilegítima de la conducta"[457].

457 **Proyecto de Ley N.º 2991/2013-CR, art. 2.-** El que deliberada e ilegítimamente accede a todo o en parte de un sistema informático, siempre que se realice con la vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa.

b. **Proyecto de Ley N.º 2999/2013-CR**, presentado el 27 de noviembre de 2013 por el congresista Mauricio Mulder Bedoya. Esta iniciativa propuso también incluir los elementos *deliberado* e *ilegítimo*. Además, sugirió suprimir el abuso de confianza como modalidad de acceso ilícito y castigar la vulneración de medidas de seguridad como figura agravada[458].

Como el lector habrá notado en la sección *legislación comparada*, ninguno de los países que se adhirieron al Convenio de Budapest recogió la fórmula aprobada por el legislador peruano, pues dicha incorporación, de un lado, reduce el ámbito de sanción y, de otro, es innecesaria. Así, la primera modificación del delito de acceso ilícito se dio el 10 de marzo de 2014, mediante la Ley N.º 30171.

5.5.4. Regulación actual

Mediante la Ley N.º 31880 se delegó facultades al Poder Ejecutivo para que legisle en materia de seguridad ciudadana, gestión del riesgo de desastres del Niño Global, infraestructura social, calidad de proyectos y meritocracia. En uso de estas facultades, el 21 de diciembre de 2023, emitió el decreto legislativo N.º 1614, a través del cual modificó los delitos de acceso ilícito y fraude informático.

¿Cuál fue el fundamento para modificar el delito de intrusismo informático? Una noticia periodística que involucraba la modificación de la base de datos de la Policía Nacional y los servicios ilegales ofrecidos a través de un grupo de Telegram:

> Según los últimos reportes periodísticos se demuestra la facilidad que tienen determinadas personas para ingresar y modificar denuncias en el sistema de seguridad de la Policía Nacional del Perú. Es así que un reportero de un determinado medio periodístico se percató que

---

Será reprimido con la misma pena, el que accede a un sistema informático excediendo lo autorizado.

458 **Proyecto de Ley N.º 2999/2013-CR, art. 2.-** El que accede de manera deliberada e ilegítima a todo o en parte de un sistema informático, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa. Será reprimido con pena privativa de libertad de tres a cinco años y con noventa días-multa siempre que el delito se realice con la vulneración de medidas de seguridad establecidas para impedirlo.

mediante la red social Telegram ha advertido una suerte de bandas criminales cibernéticas que operan para realizar, por ejemplo, denuncias policiales, requisitorias, hackeo de WhatsApp, deudas bancarias, entre otros servicios ilícitos, ofreciendo sus servicios por 45.00 soles para colocar por ejemplo una denuncia policial a una persona por robo agravado a mano armada.

Del mismo modo, la página web del INDECI fue reportada como maliciosa por un proveedor de seguridad. Un experto especialista de ESET Perú señaló [lo siguiente:] "Esto quiere decir que ciberdelincuentes tuvieron acceso al servidor o a la página web de la institución". ¿Cómo han podido tener acceso a esto? Probablemente, haya podido vulnerar cierta página, de tal manera que cualquier persona que intente ingresar tiene la posibilidad de descargar este *script* en su equipo.

Ante el incremento de los delitos de cibercriminalidad, por precisamente vulnerar los sistemas de seguridad, se propone modificar el artículo 2 de la Ley N.º 30096, incorporando como agravante el supuesto del agente que accede deliberadamente e ilegítimamente, en todo o en parte, al sistema informático vulnerando las medidas de seguridad establecidas para impedirlo, ello con la finalidad de reprimir penalmente con mayor intensidad a aquellas personas que vulneran las medidas de seguridad cuando una determinada institución estatal o empresa privada, cuente con tal.

En caso de que la mencionada institución o empresa no cuente con las medidas de seguridad antes señaladas y aun así el agente acceda deliberada e ilegítimamente al sistema informático, incluso, excediéndose o extralimitándose en lo autorizado, nos encontraríamos en el primer párrafo del artículo 2 de la Ley N.º 30096, que regula el acceso ilícito.

[...] En primer término, se agrega la modalidad "excederse de lo autorizado" en el tipo básico del delito de acceso ilícito; y, además, se extrae y se coloca como una modalidad agravada del tipo cuando el agente accede deliberada e ilegítimamente, en todo o en parte, al sistema informático vulnerando las medidas de seguridad establecidas para impedirlo. Para esta modalidad, se plantea una pena privativa de libertad no menor de tres ni mayor de seis años y ochenta a ciento veinte días-multa[459].

459 Poder Ejecutivo. *Decreto Legislativo N.º 1614, Decreto Legislativo que modifica la Ley N.º 30096, Ley de Delitos Informáticos, para prevenir y hacer frente a la delincuencia.* Lima: 21 de diciembre del 2023, pp. 3, 4 y 7.

Los argumentos expuestos por el Ejecutivo no justifican la modificación normativa, ya que, incluso, ni siquiera tienen relación directa con el delito de acceso ilícito, sino con otro tipo de delitos, como atentado contra los datos y sistemas informáticos:

- El Poder Ejecutivo utiliza dos artículos periodísticos de inicios del 2023: (1) "PNP: sistema de seguridad nacional es vulnerable para ciberdelincuentes"[460] -que, a su vez, recoge una investigación titulada "Destapando a la ciberdelincuencia que vulnera la seguridad de personas, negocios e instituciones"[461]- y (2) "Cómo ciberdelincuentes vulneraron seguridad del INDECI y propagaron virus con reportes de emergencia por lluvias"[462].

- **[Caso 52]** La primera noticia gira en torno a un periodista que, el 3 de mayo de 2023, acude a la comisaría de Miraflores y comprueba que no cuenta con denuncias en su contra. Luego, ingresa a un grupo de Telegram denominado Bins Perú que, a la fecha del reportaje, contaba con 10 878 miembros. El periodista contacta un usuario identificado como «Ghost», quien ofrecía subir una denuncia al sistema policial por 30 soles e ingresar una orden de requisitoria por 45 soles. Treinta minutos después de efectuar el pago, la denuncia ya estaba alojada en el sistema.

  ¿Estamos frente a un hecho que configura el delito de acceso ilícito? No necesariamente. Si el cambio normativo es de diciembre del 2023 y el reportaje se transmitió medio año antes, hubiese sido importante que el Poder Ejecutivo indagase en la

460 "PNP: sistema de seguridad nacional es vulnerable para ciberdelincuentes", en *La República*, Lima, 8 de mayo de 2023. https://larepublica.pe/sociedad/2023/05/08/pnp-sistema-de-seguridad-nacional-es-vulnerable-para-ciberdelincuentes-inseguridad-cibernetica-fraudes-ciberneticos-robos-por-internet-mdga-724528

461 "Destapando a la ciberdelincuencia que vulnera la seguridad de personas, negocios e instituciones", en Día D, Lima, 7 de mayo de 2023. https://www.youtube.com/watch?v=I_51zi77Z34

462 Miranda, Elena, "Cómo ciberdelincuentes vulneraron seguridad del INDECI y propagaron virus con reportes de lluvias", en *Convoca*, Lima 18 de marzo de 2023. https://convoca.pe/agenda-propia/como-ciberdelincuentes-vulneraron-seguridad-del-indeci-y-propagaron-virus-con

Policía o en la Fiscalía la hipótesis criminal y el estado de la investigación. Nada de eso se menciona en la exposición de motivos.

¿Por qué señalo que no estamos, necesariamente, frente a un acto que se califique como intrusismo informático? Porque, a la luz de los datos disponibles: (i) podríamos encontrarnos frente a un agente policial (usuario) que tiene acceso al sistema informático, es decir, no utiliza ninguna herramienta o técnica de vulneración de las medidas de seguridad; (ii) ingresar datos informáticos a un sistema no configura intrusismo informático (art. 2 LDI), pues es un atentado contra la integridad de los datos informáticos (art. 3 LDI), en concurso con el delito de falsedad genérica (art. 438 CP). Dicho esto, esta primera noticia no justificaba la modificación del delito de acceso ilícito.

- **[Caso 53]** La segunda noticia relata que el sistema informático del Instituto Nacional de Defensa Civil fue vulnerado y que, cada vez que un usuario daba clic a un enlace para conocer el informe y reporte de emergencia por lluvias, descargaba el troyano JS/Agent.PIV. El reportaje describe las funciones del *malware*, cómo se infectaban los usuarios y la reacción de las autoridades para solucionar este problema.

  Ahora bien, ¿es preocupante que desde una plataforma del estado peruano se esparza *malware*? Sí. ¿Configura el delito de acceso ilícito? No. Es un ataque a la integridad de un sistema informático estatal (art. 4 LDI) que potencialmente puede infectar el sistema del usuario particular. ¿Justifica la modificación del delito de acceso ilícito? No.

Como he tratado de explicar, ninguna de las dos noticias utilizadas para justificar la modificación del artículo 2 LDI cumplen su objetivo. El Ejecutivo pudo indagar sobre el número de casos que la Fiscalía archivó por no reunir el elemento *medida de seguridad* para su configuración o nuevas modalidades delictivas que surgen en nuestro país y que hayan sido identificadas por la Di-

vindat; sin embargo, perdió la oportunidad de hacerlo. Así, tenemos un delito informático modificado sin una debida explicación.

El siguiente cuadro comparativo permite identificar los cambios normativos del delito de acceso ilícito y conocer su regulación actual -que será objeto de estudio y análisis-:

Art. 2 LDI (original)	Art. 2 LDI (modificado)	Art. 2 LDI (vigente)
Fecha de publicación: 21 de octubre del 2013	**Fecha de modificación: 10 de marzo del 2014**	**Fecha de modificación: 21 de diciembre de 2023**
El que accede sin autorización a todo o parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días multa.	El que deliberada e ilegítimamente accede a todo o en parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa.	El que deliberada e ilegítimamente accede a todo o en parte de un sistema informático, o se excede en lo autorizado, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa.
Será reprimido con la misma pena el que accede a un sistema informático excediendo lo autorizado.	Será reprimido con la misma pena el que accede a un sistema informático excediendo lo autorizado.	Si el agente accede deliberada e ilegítimamente, en todo o en parte, al sistema informático vulnerando las medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa.

Cuadro 16. Regulación del delito de acceso ilícito, 2013-2024. Elaboración propia.

Con la última reforma normativa, el delito de acceso ilícito experimentó un cambio sustancial. En la actualidad, este delito se configura tanto cuando se produce un quebrantamiento de las medidas de seguridad -criterio tradicional desde 2013- como cuando no existe tal vulneración.

5.6. EL BIEN JURÍDICO PENALMENTE PROTEGIDO

Este tópico no es pacífico, pues algunos autores sostienen que se salvaguarda la intimidad personal o familiar, la intimidad informática[463], el domicilio informático o la privacidad[464]. Otros sostienen que se protege "la confidencia-

463 Lledó Benito, Ignacio. *Formas específicas de criminalidad*. Madrid: Dykinson, 2019, p. 134.

464 Sobre este punto, recomiendo el acápite denominado "Ubicación sistemática del nuevo artículo 197 bis CP e implicaciones en la determinación del bien jurídico protegido"

lidad, la integridad y la disponibilidad"[465]. Este problema interpretativo surge por la ubicación del tipo penal analizado por los juristas.

En Argentina, el *hacking* blanco o acceso ilícito sin ulterior finalidad se encuentra ubicado en el capítulo denominado *Violación de secretos y privacidad*. Esto orilla a algunos autores a considerar que "mediante el art. 153 bis del Código Penal se ampara la reserva, la confidencialidad y el derecho a la privacidad del titular del sistema y del dato informático. Este puede ser tanto una persona natural como jurídica [...] [pues] estas también tienen un derecho a la reserva y al secreto de sus papeles privados, y a la protección de sus datos personales, y hoy en día esos papeles están almacenados en su gran mayoría en ordenadores, por lo que las prohibiciones de acceso tienden a amparar estos registros informáticos"[466].

En España, de otro lado, se encuentra en el capítulo *«Del descubrimiento y revelación de secretos»*, que integra el título *De los delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad de domicilio*[467]. De ahí que sea

(Hernández Díaz, Leyre. *Los accesos ilícitos a sistemas informáticos. Normativa internacional y regulación en el ordenamiento penal español*. Navarra: Thomson Reuters / Aranzadi, 2019, pp. 269-276). También el análisis realizado sobre el art. 197 bis por Sanz Delgado, Enrique. "Delincuencia cibernética y descubrimiento y revelación de secretos". En: Sanz Delgado, Enrique y Daniel Fernández Bermejo (coords.). *Tratado de delincuencia cibernética*. Navarra: Thomson Reuters / Aranzadi, 2021, pp. 277 y s.

465 Entre ellos, Meneses Gonzáles, Bonifacio y Jean Paul Meneses Ochoa. *La cibercriminalidad: Consideración criminológica, político-criminal, dogmática, procesal y cooperación internacional*. Salamanca: UPSA, 2024, p. 305. En la misma línea, García León, "Análisis del tipo de acceso ilícito. Bien jurídico, tipicidad objetiva y subjetiva, autoría y participación, y su distinción con el delito de atentado a la integridad de datos y sistemas informáticos", cit., pp. 362-365.

466 Palazzi, Pablo A. "El delito de acceso ilegítimo a un sistema informático". En: Dupuy, Daniela (dir.). *Cibercrimen II. Nuevas conductas penales y contravencionales. Inteligencia artificial aplicada al derecho penal y procesal penal. Novedosos medios probatorios para recolectar evidencia digital. Cooperación internacional y victimología*. Buenos Aires: B de F, 2018, p. 41.

467 Algunos autores españoles analizan el bien jurídico por el capítulo antes que por el título en el que se encuentra ubicado: "La aportación esencial de esta última reforma del Código Penal es la reubicación del precepto en el nuevo art. 197 bis, modificación que merece una valoración positiva y facilitará sin duda una más adecuada interpretación del tipo penal, al quedar configurado al margen de las figuras delictivas que protegen específicamente el derecho a la intimidad. Tal y como se

importante conocer su ubicación en el ordenamiento penal para analizarlo adecuadamente y delimitar su objeto de protección. La ubicación del delito bajo análisis en la legislación española ha llevado a proponer que ciertas conductas deben ser excluidas:

> El legislador español ha decidido introducir el precepto entre los delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, ubicación errónea para quienes defendemos que lo protegido es un bien jurídico colectivo antepuesto: la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, o si se prefiere, y de forma abreviada, pero teniendo en cuenta que con ellos se hace referencia a las condiciones en las que se respetan los atributos anteriores, la seguridad informática [...]. Por ello, algunos autores han propuesto crear un título nuevo en el Código penal que llevara por rúbrica "Delitos contra los sistemas de información".
>
> [...]
>
> Pero los problemas de la incorrecta ubicación sistemática no acaban aquí. La doctrina se pregunta también si al estar este delito dentro de los dedicados a proteger la intimidad personal y familiar, una interpretación sistemática obliga a considerar atípicas, no delictivas, las intromisiones en sistemas informáticos que no contengan datos de esta clase [...] La postura de la Fiscalía, sin embargo, parece ser la contraria,

---

define la conducta, el acceso ilegal a un sistema informático no tiene por qué implicar atentado alguno contra la intimidad, pues la consumación del delito no exige el conocimiento o apoderamiento de datos personales o información sobre individuos concretos y determinados. Estamos, en definitiva, ante un precepto que, como se ha indicado, protege básicamente la seguridad de los sistemas informáticos o incluso el uso reservado de los mismos, pero no la intimidad o la privacidad como derechos fundamentales de las personas" (Tejada De La Fuente, Elvira. "Novedades en la tipificación de determinados delitos vinculados a la criminalidad informática en el Código Penal español: evolución legislativa y adaptación a la normativa internacional". En: Dupuy, Daniela [dir.] y Mariana Kiefer [coord.]. *Cibercrimen. Aspectos de derecho penal y procesal penal. Cooperación internacional. Recolección de evidencia digital. Responsabilidad de los proveedores de servicios de Internet*. Montevideo: B de F, 2019, pp. 47 y s.). De otro lado, "[e]l bien jurídico que protegen -dada la ubicación del precepto en el título señalado- es la intimidad y privacidad individual que encarnan la finalidad protectora que persigue el tipo penal, al blindar el ámbito propio y reservado del individuo frente a la acción y el conocimiento de los demás" (Velasco Núñez, *Delitos tecnológicos. Cuestiones penales y procesales*, cit., p. 222).

> pues en su Circular 3/2017 afirma que el acceso ilegal a un sistema informático castigado en el art. 197 bis puede cometerse también para acceder a secretos de empresas o a secretos oficiales. Es decir, no lo reduce al ataque a sistemas que contengan datos personales y familiares. En esta obra vamos a defender que esta es la solución correcta, pues es coherente, además, con la exposición de motivos de la reforma de 2015, que remite a los compromisos internacionales, y se refiere expresamente a la intención de incluir supuestos que no afectan a la intimidad personal[468].

Regresando al Perú, como recordará el lector, el artículo 207-A CP -que tipificó la primera modalidad de acceso ilícito en nuestro ordenamiento, hacia el 2000- se incorporó al Título V de la Parte Especial ("Delitos contra el patrimonio") del Código Penal, lo que dificultó comprender su objeto de protección. Esto se superó en el 2013, ya que el legislador lo ubicó en el Capítulo II ("Delitos contra datos y sistemas informáticos") de la LDI.

Cierto sector de la doctrina nacional considera que el bien jurídico protegido es la integridad informática, "entendiendo a esta como el conjunto de datos o sistemas informáticos que debieran mantenerse incólumes e intactos ante intentos de acceso que no son permitidos o resultan ilegítimos"[469]. Considero que no es así, pues Perú sanciona el mero intrusismo o *hacking* blanco, es decir, no se exige que el ciberdelincuente haya ocasionado algún daño o generado algún peligro. En caso de que la integridad informática fuese mermada, ya no nos encontraríamos frente al delito bajo estudio, sino ante los previstos en los artículos 3 y 4 de la LDI.

Personalmente, en atención a la ubicación del delito estudiado, su naturaleza –es un ciberdelito puro–, así como la adhesión del Perú al Convenio de Budapest[470], considero que se protege la seguridad informática[471], de manera

468 Gil Gil/Hernández Berlinches, *Cibercriminalidad,* cit., p. 197-199.

469 Arévalo Minchola/Vega Aguilar, *Ciberdelitos. Análisis en el sistema penal,* cit., p. 255.

470 Council of Europe. *Convenio sobre la ciberdelincuencia,* Budapest, 23 de noviembre de 2001. https://www.oas.org/juridico/english/cyb_pry_convenio.pdf. El Convenio incluye el delito de acceso ilícito en el título de delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos.

471 En la misma línea, Jiménez Herrera, *Manual de derecho penal informático,* cit., p. 404. "El bien jurídico protegido es la seguridad de los sistemas informáticos, puesto

general, y la **confidencialidad** de los datos y sistemas informáticos, de forma específica[472]. En efecto, los delitos ubicados sistemáticamente en el primer capítulo de la LDI sancionan los actos cometidos contra tres propiedades de la seguridad informática: confidencialidad, integridad y disponibilidad[473]. No

---

que se sanciona al que accede a los sistemas informáticos vulnerando las normas de seguridad" (Rodríguez Rocha, Lizet Nancy. "El delito de acceso ilícito a los sistemas informáticos. Análisis del tipo penal y el rol de la cooperación judicial internacional". En: Espinoza Calderón, Víctor Raúl [coord.]. *Cibercriminalidad y delitos informáticos*. Lima: Instituto Pacífico, 2023, p. 339). "Desde nuestro particular punto de vista la información vendría a ser aquella que se encuentra siendo protegida, pero no cualquier información o cualquier expresión de la información, sino aquella que se encuentra contenida en algún sistema o dato informático. De ahí que se apuntaba cuando analizábamos los delitos informáticos extintos en nuestro país, la existencia de un bien jurídico adicional al patrimonio y lo denominábamos "seguridad informática". (Arévalo Minchola/Vega Aguilar, *Ciberdelitos. Análisis en el sistema penal*, cit., p. 254).

472 "Desde nuestro punto de vista, esta es la línea correcta para definir el bien jurídico protegido en la tipificación de las conductas que consisten en un acceso ilícito a sistemas informáticos, si bien es cierto que es necesario distinguir, por un lado, la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos y, por otro lado, de los datos propiamente dichos [...] El bien jurídico aludido y que se refiere a la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos constituye una barrera de contención de riesgos para otros bienes jurídicos que se pueden encontrar involucrados en la función social que desempeñan tales sistemas y redes informáticas: la intimidad personal y familiar, el patrimonio, etc." (Rueda Martín, María Ángeles. "Cuestiones político-criminales sobre las conductas de *hacking*". En: *Derecho Penal Contemporáneo. Revista Internacional* 28. Bogotá: 2009, pp. 175 y 179). En la misma línea: "Por nuestra parte, entendemos que la tutela penal debe estar orientada a la confidencialidad de los datos [...] Nótese que la materia de prohibición se erige sobre el presupuesto de la reserva de los datos almacenados en el sistema informático. Ello se deduce de manera taxativa del grado de accesibilidad a los datos, es decir, acceso al sistema o dato informático debe ser de carácter restringido" (Aboso, *Derecho penal cibernético*, cit., p. 181).

473 En esta línea, Víctor Espinoza (*Delitos informáticos y nuevas modalidades delictivas*, cit., p. 70) sostiene que se protege la "ciberseguridad". Sobre este punto, "la legitimidad del tipo penal que proscribe dichas acciones se evidencia una vez que la mencionada disposición es entendida como la prohibición de acceder a la seguridad de la información contenida en los sistemas de tratamiento automatizado de datos, que justamente es el bien jurídico tutelado, advertido el particular contexto generado a raíz del apresurado desarrollo de las tecnologías de la información y de la comunicación (era de la informática)" (Palomino Ramírez, Walter. "El intrusismo y los otros delitos informáticos regulados en la Ley N.º 30096". En: *Gaceta Penal*

obstante, el acceso ilícito protege específicamente la confidencialidad[474], en tanto que los atentados contra los datos y sistemas informáticos hacen lo propio con su integridad y disponibilidad.

Entre los autores que consideran que la seguridad informática es el bien jurídico protegido, se encuentra la profesora Montserrat Sánchez Escribano, quien precisa que se presenta un carácter supraindividual, pero que tiene una estrecha relación con otros bienes jurídicos a los que ofrece protección mediata, lo que no impide afirmar su autonomía:

> La seguridad informática es, pues, un bien jurídico supraindividual de carácter puro, ello por su contenido, ya que resulta indispensable para garantizar el funcionamiento del sistema teniendo como función la satisfacción de las necesidades sociales y que se encuentra vinculado a la protección de distintos derechos de corte individual y colectivo.
>
> La seguridad informática comprende, en consecuencia, el ejercicio de determinadas condiciones de seguridad para el funcionamiento de sistemas y para el goce tranquilo de determinados derechos o bienes individuales. Brinda protección en otros ilícitos con un mayor contenido de injusto. Así pues, se trata de un bien jurídico de sujeto múltiple del que nadie puede disponer y cuya manifestación colectiva se manifiesta

---

& Procesal Penal 56. Lima: 2014, p. 139). "Desde ya, puede señalarse que el acceso ilícito, el atentado a la integridad de datos o sistemas informáticos (ars. 3 y 4), la interceptación de datos informáticos (art. 7), y el abuso de mecanismos y dispositivos informáticos (art. 10) se destinan a la protección de la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos. Así lo indica el apartado 43 del IECC" (Oré Sosa, *Delictum. Apuntes de derecho penal*, cit., p. 191). "Son delitos que protegen más que la información, la seguridad de la información, en la creencia de que hoy en día, es a través de estas tecnologías que protegemos nuestra privacidad frente a terceros" (Velasco San Martín/Velázquez, *Aspectos prácticos de los ciberdelitos y la evidencia digital,* cit., p. 180).

474 "Esta figura penal de acceso ilícito sanciona la violación de la confidencialidad, que se realiza a través del acceso no autorizado al sistema, vulnerando las medidas de seguridad establecida para evitar que ajenos ingresen a un sistema informático; por el verbo rector acceder se entiende el hecho de entrar en un lugar o pasar a él, que en esta figura se entiende el acto de entrar sin autorización del titular a un sistema" [el subrayado es mío] (Villavicencio Terreros, "Delitos informáticos", cit., p. 291).

además en la existencia de un interés particular en cada uno de los sujetos implicados[475].

Como se puede apreciar, su protección radica en la necesaria anticipación de la tutela penal tanto de bienes jurídicos de naturaleza individual como de interés de índole colectivo[476].

5.7. EL TIPO PENAL DE ACCESO ILÍCITO

El Convenio de Budapest propuso una fórmula básica de acceso ilícito: "El acceso deliberado e ilegítimo a todo o parte de un sistema informático", dejando a cada Estado parte la facultad de exigir que el delito se cometa:

(i) infringiendo medidas de seguridad;

(ii) con la intención de obtener datos informáticos y otra intención delictiva; y

(iii) en relación con un sistema informático conectado a otro sistema informático.

Perú, en la adhesión del 2019, declaró que nuestra LDI "exige que el delito de acceso ilícito se cometa infringiendo medidas de seguridad"; es decir, precisó que los elementos (ii) y (iii) no integran la configuración de nuestro tipo penal. Sin embargo, como ya he mencionado, esto cambió en diciembre

475 Montserrat Sánchez-Escribano, María Isabel. *El delito de acceso ilícito a un sistema informático: aspectos relativos a su regulación e interpretación*. Navarra: Thomson Reuters / Aranzadi, 2022, pp. 151 y s.

476 La misma autora detalla una relación no exhaustiva, pero sí pedagógica de los bienes que, de forma mediata, pueden ser protegidos a través del delito bajo estudio: "En mi opinión, en el delito de acceso ilícito a un sistema informático pueden verse mediatamente afectados los siguientes bienes jurídicos la intimidad, la propia imagen, el honor, el patrimonio, el orden socioeconómico (y, dentro de éste, la propiedad intelectual, la propiedad industrial y los intereses relativos al mercado y a los consumidores como el secreto de empresa), en ciertos casos también la Administración de Justicia y la Administración pública, el tráfico jurídico (falsedades), los intereses del Estado (seguridad nacional), la libertad de culto, de conciencia e ideológica y la libertad de información" (Montserrat Sánchez-Escribano, *El delito de acceso ilícito a un sistema informático: aspectos relativos a su regulación e interpretación*, cit., pp. 152 y s.).

del 2023, al modificar el tipo penal y dejar de exigir el elemento (i) -en la configuración básica-.

De esta forma, la actual tipificación del delito de acceso ilícito en la legislación penal peruana recoge la siguiente configuración:

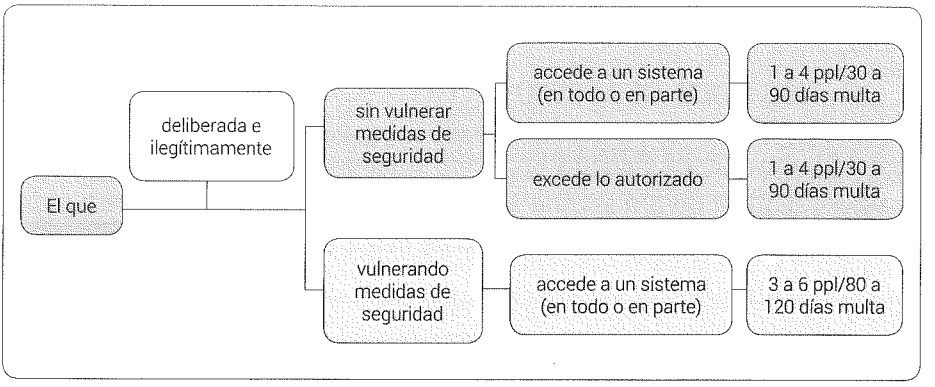


Diagrama 7. Estructura actual del delito de acceso ilícito, en el sistema penal peruano. Elaboración propia.

Como se puede observar, el actual artículo 2 LDI sanciona el acceso ilícito cometido, incluso sin la vulneración de medidas de seguridad. Tampoco exige motivación delictiva adicional. En otras palabras, no requiere un elemento subjetivo distinto del dolo. En un artículo publicado en junio del 2014, cuestioné esta opción legislativa y mantengo mi posición: debería exigirse esa finalidad adicional que, incluso, es sugerida como opción por el Convenio de Budapest. No toda lesión al bien jurídico protegido debe traer la misma respuesta estatal: ¿por qué debemos acudir al derecho penal frente a cualquier intrusismo informático? Lo graficaré con algunos ejemplos, sin embargo, le pido al lector que elimine de su mente aquellos accesos ilícitos que tienen una finalidad delictiva posterior, pues ese tipo de acciones sí merece reproche penal y, precisamente, es lo que postulo desde la promulgación de la LDI:

- **[Caso 54]** Algunos *smart* TV permiten proteger el acceso con una contraseña, es decir, si no cuentas con la clave, no podrás utilizarlo para ver televisión. Ahora bien, pensemos en el siguiente caso: A es el jefe de un estudio jurídico y ha colocado una contraseña a todos los televisores de su oficina. B adivinó

la clave *12345* y, cada vez que A se retira a almorzar, B y sus compañeros ven televisión en el directorio. ¿Por qué B debe ser reprimido penalmente? ¿Acaso no sería suficiente con despedirlo o amonestarlo?

- [**Caso 55**] C y D son compañeros de departamento. C se encuentra muy molesto con D, pues desde que amanece permanece absorto en su Play Station 5 (PS5) y no realiza las tareas de limpieza que han acordado. Pese a que han charlado en más de una oportunidad, su conducta es igual. Entonces, C ha colocado una clave de inicio de sesión a su PS5. D, al tercer intentó, adivinó la contraseña: 0000. Es así como logra ingresar y seguir jugando. ¿El derecho penal debe intervenir para sancionar esta actuación?

- [**Caso 56**] E es alumno del curso de Bases Romanistas del Derecho. Se encuentra muy angustiado, pues no sabe cómo le fue en la evaluación escrita. Cuando su profesor F va por un café, E ve un *post it* pegado en el teclado con la contraseña de acceso. Rápidamente ingresa al ordenador y ve su calificación, luego de lo cual cierra sesión. ¿No será suficiente el castigo que reciba por parte de su universidad?, ¿por qué deber ser reprimido penalmente?

- [**Caso 57**] G y H son novios. El último fin de semana hicieron senderismo en las Lomas de Lachay. Al llegar a casa, G "cayó rendido" y olvidó enviarle las fotografías que tomó con su celular a H. Esta última, para no despertarlo, desbloqueó el celular con la huella de G mientras dormía. Revisó las fotografías y apagó el celular -feliz por las tomas que habían conseguido-. ¿H es una ciberdelincuente? ¿La unidad especializada de la policía y la fiscalía fueron creadas para investigar este tipo de casos?

En estos cuatro ejemplos tenemos: (1) sistemas informáticos -*smart* TV, PS5, computadora, teléfono celular-, (2) medidas de seguridad quebradas

-contraseñas-, (3) ausencia de consentimiento para el ingreso o acceso y (4) voluntad para ingresar a un sistema sin autorización. Tal y como se encuentra redactado nuestro tipo penal, los cuatro casos se subsumen en la modalidad agravada del artículo 2 LDI. Estos ejemplos son casos de *mero intrusismo*, pues no importa la finalidad por la que ingresó el sujeto activo, ya que se castiga el simple acceso indebido. Mi crítica no busca despenalizar el delito de acceso ilícito, sino incluir la finalidad delictiva posterior, es decir, tipificarlo como un delito de tendencia interna trascendente[477] -hasta que no ocurra un cambio legislativo, se deberá acudir al principio de lesividad al analizar este tipo de casos para evitar la sobrepenalización-.

En nuestro país, no se exige que el acceso se realice de forma remota -como los ejemplos antes descritos lo reflejan-. Aunque esta característica es importante, desde un punto de vista criminológico, la mayoría de las legislaciones locales no ha incluido este requisito:

> En todo caso, el *hacking* es siempre, por su propia naturaleza, un acceso remoto, esto es, realizado a distancia por el sujeto que, normalmente a través de Internet, se entromete en un sistema sin tener contacto físico con él. No es *hacking* propiamente dicho el acceso directo, en la propia terminal, y no autorizado a un sistema informático. Este comportamiento, usual en el ámbito familiar o laboral y generalmente realizado para obtener información sensible que puede estar contenida en el sistema, no puede considerarse *hacking* a efectos criminológicos, puesto que sus características de riesgo son distintas a las del acceso

477 El jurista peruano Eduardo Oré Sosa también advierte algunos problemas al castigar actuaciones de escasa potencialidad lesiva, "por el solo afán de superar un reto personal o para evidenciar la especial vulnerabilidad de los sistemas informáticos (agujeros) de algunas entidades públicas o privadas. Habrá que ver si, en casos como estos, puede excluirse la imputación apelando al criterio de la disminución del riesgo. En cualquier caso, no pasarán de constituir supuestos marginales o excepcionales, más aún si se concibe esta figura como un delito de mera actividad que se consuma en el momento mismo en que se vulnera la medida de seguridad" (Oré Sosa, *Delictum. Apuntes de derecho penal*, cit., p. 193). Sobre el mero intrusismo, también: "Finalmente, parece que la tipificación quiere ser más incriminante, en tanto no se exige, como lo hacía la legislación anterior, un propósito ulterior, que no tenía que manifestarse en el mundo fenoménico para dar por realzada la acción típica" (Peña Cabrera Freyre, Alonso. "Los delitos informáticos: el uso de instrumentos digitales en las redes informáticas y en el ciberespacio". En: *Gaceta Penal & Procesal Penal* 76. Lima: 2015, p. 161).

> informático ilícito realizado en el ciberespacio. Es evidente, en todo caso, que tal forma de *hacking* cuyo análisis no interesa aquí, sí constituirá un acceso ilícito a un sistema informático conforme a la regulación jurídica de la mayoría de los países[478].

Cierto sector de la doctrina nacional considera que el fundamento político criminal de este delito radica en ser el paso previo "obligatorio" para atentar contra sistemas informáticos[479]. Discrepo respetuosamente de esta posición, por dos razones:

a. No es la opción legislativa adoptada en Perú. Me explico, quienes consideran que el delito de acceso ilícito facilita la comisión de otros delitos, están pensando en una fórmula legislativa distinta a la que se recoge en la LDI, es decir, no en el *mero intrusismo*, sino en el *acceso ilícito como delito de tendencia interna trascendente* -que es la propuesta legislativa más adecuada, desde mi perspectiva, pero no la recogida en nuestro país-. Bajo esta mirada, no se castigaría el acceso ilícito por el solo hecho de ingresar, sino por ingresar con una intención delictiva adicional.

b. No se necesita acceder ilegalmente a un sistema informático para atentar contra este. Por ejemplo, puedo enviar por correo electrónico un *malware*, *software* dañino, infectarlo y perjudicar el

---

478 Miró Llinares, *El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio*, cit., p. 54.

479 "La tipificación tiene fundamento criminológico: Al analizar la ciberdelincuencia, se analiza también la modalidad criminal y en el caso de sistemas informáticos, todo acto de alteración, daño y/o modificación de este va a partir de un acceso ilícito como primer acto". Los autores continúan afirmando: "Esto es, para la comisión del delito de atentado contra la integridad de sistemas informáticos, obligatoriamente se debe haber dado un acceso ilícito. Pero dentro de esta secuencia criminal, entonces, existe justificación tanto para criminalizar el atentado concreto de sistemas informáticos, así como el simple acceso ilícito, ya que en este último caso lo que se penaliza no es la modificación o destrucción del sistema, sino el solo hecho de penetrarlo de manera ilegítima. El fundamento criminológico tendrá una forma de adelantamiento de la barrera de punición, entendiendo que no se puede dejar impune ninguna de las secuencias que recorre el plan criminal del ciberdelincuente para hacerse con datos y partes de un determinado sistema informático" (Arévalo Minchola/ Vega Aguilar, *Ciberdelitos. Análisis en el sistema penal*, cit., pp. 251 y s.). Para Eloy Velasco (*Delitos tecnológicos. Cuestiones penales y procesales*, cit., p. 217) es el "delito medio para cometer otros (mediante virus troyanos, *botnets*, *spyware*, *keyloggers*, etc.)".

funcionamiento del sistema informático sin haber accedido ilegalmente. De la misma forma, puedo acceder ilegalmente con una finalidad ilegal sin llegar a cometer otro delito. Es por esta razón que considero inadecuado afirmar que el delito de acceso ilícito es el paso previo de otro delito: Habrá casos en que esto suceda, pero también otros en los que no. Tratémoslos como delitos independientes que, en algunas ocasiones, confluirán.

5.7.1. Elementos comunes

5.7.1.1. Sujetos

El **sujeto activo** puede ser cualquier persona, ya que el tipo penal no exige que cuente con funciones o características especiales. Debemos evitar suponer que este tipo de delito es cometido por personas que poseen conocimientos especializados, pues no necesariamente es así[480].

De este modo, cierto sector de la doctrina nacional reconoce que nos encontramos frente a un delito común, pero sugiere que el agente cuenta con conocimientos técnicos especiales que le permite cometer este delito:

> [...] Nos encontramos ante un delito común, toda vez que el tipo penal no exige ninguna cualidad especial, razón por la cual el sujeto activo en el delito de acceso ilícito, en principio, va a ser cualquier persona; no obstante, por la exigencia para el manejo de la informática, es necesario que el sujeto activo tenga las condiciones técnico-suficientes para el conocimiento y uso de la informática.
>
> De otro lado, el sujeto activo será cualquiera que se encuentre dentro de la clasificación de la delincuencia informática; específicamente los agentes comunes que cometen estos tipos de ilicitudes son los *hackers* (personas que tienen conocimientos en el manejo de la informática). Porque si nos adelantamos al análisis del comportamiento que exige este tipo penal, podemos advertir que consiste en un conjunto de

480 Al analizar la reforma legislativa argentina, Sueiro destaca que no se recurrió a categorías criminológicas propias de la cibertipología como *hacker, cracker, preaker* o *phreaker, phisher, sniffer, virucker,* propagandista informático, pirata informático o *cyberbullyng* o ciberacosador (Sueiro, Carlos Christian. *El derecho penal en la era digital. Delincuencia informática. Criminalidad informática. Prueba digital. Vigilancia electrónica. Pedagogía en la era digital.* Lima: A&C Ediciones Jurídicas, 2018, pp. 46 y s.).

> comportamientos de acceso o interferencia no autorizados, de forma subrepticia, a un sistema informático o red de comunicación electrónica de datos y a la utilización de los mismos sin autorización o más allá de lo autorizado. Este conjunto de conductas, son realizadas por los *hackers*, además que estos sujetos la doctrina los ha determinado con el apelativo: "los curiosos de la informática"[481].

En general, la doctrina local se orienta a identificar o resaltar el conocimiento técnico especializado y asociarlo como rasgo o característica de este tipo de ciberdelincuentes:

> Su comisión requiere de un agente que tenga un buen dominio de la materia, ya que estos conocimientos son aprovechados para cometer o cooperar con la comisión de delitos. En algunos casos dicha actividad persigue fines de lucro, en otras es tomado solamente como un reto de competencia entre *hackers*. Existen grupos de aficionados que se dedican a *hackear* en nuestro país, como, por ejemplo, determinados grupos de *gamers* o jugadores de videojuegos en línea que eventualmente realizan *hacking* como entretenimiento[482].

No comparto esta posición, pues, de un lado, no se requieren conocimientos tecnológicos avanzados para su comisión -recordemos los ejemplos que desarrollé líneas atrás- y, de otro, se estigmatiza a la comunidad *hacker*. Dicho de otro modo, cualquier persona, con o sin conocimiento técnico especializado, puede cometer este delito.

En el argot tecnológico, por ejemplo, se denomina *scriptkiddies*, a quienes no cuentan con habilidades especializadas, pero que utilizan programas, *scripts* o códigos ya diseñados para cometer actos ilícitos. En general, en la comunidad *hacker*, es un término utilizado de forma despectiva[483].

---

481 Jiménez Herrera, *Manual de derecho penal informático*, cit., pp. 405 y s.

482 Espinoza Calderón, *Delitos informáticos y nuevas modalidades delictivas*, cit., p. 73.

483 "Jóvenes que, no siendo expertos *hackers* capaces de acceder a sistemas mediante programaciones propias, realizan sus ataques informáticos, generalmente eligiendo las víctimas al azar, aprovechando programas y scripts básicos y causando daños en muchos casos, más fruto de su impericia o de la dañosidad del *malware* utilizado, que de sus habilidades" (Miró Llinares, *El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio*, cit., p. 307). Por su parte, Caballero y Cilleros afirman lo siguiente: "Se trata de un término despectivo para definir a un atacante inexperto que

El **sujeto pasivo** es el titular del sistema informático, cuya confidencialidad ha sido vulnerada[484]. Así, puede ser tanto una persona natural como una persona jurídica.

No debe confundirse el propietario del dispositivo con el titular del sistema informático. Por ejemplo, en casa se suele tener una computadora familiar con varias cuentas asociadas (abuelo, mamá, papá, hijo mayor, hijo menor, etc.) En este caso, si alguien accede ilegalmente a la cuenta del hijo mayor, será este el sujeto pasivo, por más que sus padres hayan adquirido el ordenador.

También debe diferenciarse el titular del sistema informático del titular de los (posibles) datos personales contenidos en el sistema[485]. Por ejemplo, si un ciberdelincuente ingresa al sistema informático de una universidad y logra acceder a bases de datos que contienen información de estudiantes, será la universidad el sujeto pasivo del acceso ilícito y no su plana estudiantil.

[Caso 58] En noviembre de 2024, el actor de amenazas Nam3L3ss publicó más de 2,8 millones de líneas de datos de empleados de Amazon, incluido sus nombres de contacto, direcciones de correo electrónico y ubicaciones en las oficinas. En diversos foros, se ubicaron datos similares de otras empresas: Lenovo, HP, TIAA, Schwab, HSBC, Delta, Metlife, etc. Poco tiempo después, se dio a conocer que el ataque no se dirigió contra los sistemas informáticos de Amazon, sino contra los de una empresa proveedora de servicios que almacenaba cierta información de las compañías afectadas: MoveIt Transfer[486].

---

es capaz de ejecutar un script o una aplicación (desarrollada por otros) para llevar a cabo un ataque. Los script kiddies normalmente no tienen un alto nivel de programación o conocimiento de las aplicaciones que usan, por lo que, cuando sus ataques han concluido, dejan muchas huellas y se les puede rastrear con facilidad" (Caballero, María Ángeles y Diego Cilleros Serrano. *El libro del hacker. Edición 2022*. Madrid: Anaya, 2022, p. 39).

484 "En efecto, sujeto pasivo será aquel que ejerce la titularidad sobre el derecho de acceso al dato o al sistema informático" (Jiménez Herrera, *Manual de derecho penal informático*, cit., p. 407).

485 "De esta suerte, el acceso ilícito al sistema informático de una entidad privada tendrá por sujeto pasivo a la empresa, no a los clientes cuya información ha quedado expuesta" (Oré Sosa, *Delictum. Apuntes de derecho penal*, cit., p. 193).

486 Centro Nacional de Seguridad Digital. Alerta integrada de seguridad digital N.º 260-2024. Lima: 11 de noviembre de 2024, p. 4. https://www.gob.pe/institucion/pcm/informes-publicaciones/6169391-alerta-integrada-de-seguridad-digital-n-260-2024-cnsd

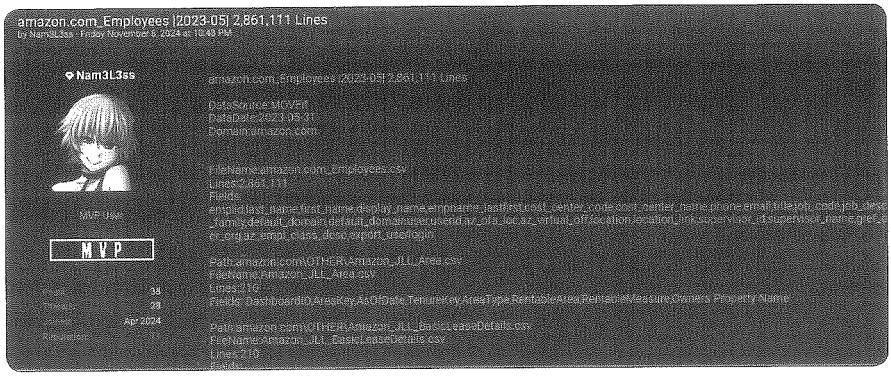


Imagen 11. En diversos foros, el actor de amenazas informó que contaba con casi tres millones de registros de Amazon, entre otras empresas[487].

Este ejemplo grafica que el sujeto pasivo del delito de acceso ilícito no tiene que ser necesariamente el propietario de los datos afectados.

5.7.1.2. Tipo subjetivo

Al analizar la tipicidad subjetiva, se aprecia que este delito no admite figuras culposas, es decir, solo puede ser cometido **dolosamente**. Además, se precisa que se debe actuar **deliberadamente** -elemento que se encuentra enlazado con el fuero interno del agresor-. De esta manera, la redacción descartaría no solo las conductas culposas sino también las que se ejecuten con dolo eventual. Como ya he adelantado, considero que es un desacierto que generará problemas de aplicación.

Al analizar el aspecto subjetivo, el profesor Oré Sosa puntualiza que "el legislador exige que el acceso ilícito sea deliberado. Esto suele entenderse como dolo directo. Se trata de un requisito que en modo alguno restringe el ámbito de la aplicación del tipo, pues la necesidad de que se vulnere una específica medida de seguridad torna irrelevante tal exigencia"[488]. Es importante precisar

487 La imagen fue obtenida de: Help net security. *Massive troves of Amazon, HSBC employee data leaked*, publicado el 12 de noviembre de 2024. https://www.helpnetsecurity.com/2024/11/12/amazon-employee-data-leaked/

488 Oré Sosa, *Delictum. Apuntes de derecho penal*, cit., p. 193. En una línea similar: Almanza Altamirano, Frank. *Cibercriminalidad y nuevas modalidades delictivas*. Lima: San Bernardo, 2024, p. 64. Para este autor, el delito de acceso ilícito se configura únicamente mediante una actuación con dolo directo.

que este análisis se realizó antes de la modificación de diciembre del 2023, esto es, cuando la vulneración de medidas de seguridad era un elemento esencial para la configuración del delito. Hoy, ya no es así. En consecuencia, es necesario delimitar los alcances del elemento *deliberadamente*.

Vega Aguilar y Arévalo Minchola, por otro lado, sostienen que "el delito de acceso ilícito sin la incorporación del término *deliberadamente* no significaría dolo directo. En base a la técnica legislativa, estaría exento de la expresión *a sabiendas* y su descripción típica daría lugar a colocar casos tipos donde la inexactitud de las autorizaciones o situaciones análogas nos podría hacer ver dificultad en la interpretación del dolo eventual. Así, entonces, consideramos que la introducción del término *deliberadamente* ha venido a complementar el aspecto subjetivo, dotando con claridad la exigencia de presentación de dolo directo para la comisión del referido delito"[489].

Se debe recordar que los términos deliberada e ilegítimamente se incluyeron en la modificación de la LDI -adhesión sugerida en los proyectos de ley 2991/2013-CR y 2999/2013-CR-, pues, según los proponentes, nuestra legislación no cumplía con los estándares previstos en el Convenio de Budapest. No obstante, si revisamos el párrafo 39 del Informe Explicativo del citado instrumento, veremos que se sugirió que la conducta sea deliberada, entendiéndola como dolosa -y no para precisar qué grado de conocimiento deben exigir los Estados, como cierto sector de la doctrina nacional interpreta-:

> Todos los delitos contenidos en el Convenio deben ser cometidos de manera "deliberada" para que se aplique la responsabilidad penal. En ciertos casos, un elemento deliberado específico forma parte del delito. Por ejemplo, en el artículo 8 que trata del delito de fraude informático, la intención de obtener un beneficio económico es un elemento constitutivo del delito. Quienes redactaron el Convenio llegaron al acuerdo de que el significado exacto del término "deliberado" debería ser interpretado conforme a las leyes de cada país.

489 Arévalo Minchola/Vega Aguilar, *Ciberdelitos. Análisis en el sistema penal*, cit., pp. 263 y s.

Es más, si revisamos la legislación de los países latinoamericanos que se adhirieron al Convenio de Budapest, veremos que ninguno ha incluido los términos *deliberada* e *ilegítimamente* en su redacción.

Al igual que el profesor Peña Cabrera Freyre, considero que al incorporar el elemento *deliberadamente*, el legislador acuñó una valla innecesaria que genera problemas de interpretación y aplicación:

> La expresión "deliberadamente" en el tipo subjetivo del injusto es una valla que el legislador no debió colocar. El dolo es consciencia y voluntad de la realización típica, de manera que -a nuestro entender- basta que el agente sepa con rayana exactitud que está invadiendo una base de datos ajena para dar por confirmado el tipo penal [...]. Al constituir un elemento subjetivo del injusto ajeno al dolo, debe graficar algo distinto a este último, situación que no apreciamos en el tipo penal, pues dicho elemento no dice nada distinto al dolo, por lo que lo único que va a generar es problemas interpretativos, ya que algunos pretenderán argumentar que la intención no fue intencional. En una propuesta de *lege ferenda* este elemento debe ser excluido de la composición típica en cuestión[490].

En esta misma línea crítica, Pérez López opina que:

> La expresión "deliberadamente" en el tipo subjetivo del injusto es una valla que el legislador no debió colocar. El dolo es consciencia y voluntad de la realización típica, de manera que, a entender de Mazuelos Coello, basta que el agente sepa con rayana exactitud que está invadiendo una base de datos ajena para dar por confirmado el tipo penal. Y es que el término "deliberado" tiene que ver con un acto *ex profeso* del autor, con una intención determinada o propósito de generar un cierto estado de desvalor. Al constituir este un elemento subjetivo del injusto ajeno al dolo, de acuerdo con Peña Cabrera Freyre, debe graficar algo distinto a este último, situación que no se apreciaría en el tipo penal, pues dicho elemento no dice nada distinto al dolo, por lo que lo único que podría generar serían problemas interpretati-

490 Peña Cabrera Freyre, "Los delitos informáticos: el uso de instrumentos digitales en las redes informáticas y en el ciberespacio", cit., p. 161.

> vos, ya que algunos pretenderán argumentar que la intrusión no sería "intencional"[491].

En diferentes escenarios académicos he manifestado mi posición, la cual es crítica a la redacción actual: no podemos ignorar que la conducta, además de ser dolosa, debe ser deliberada; sin embargo, nuestra interpretación ha de maximizar sus alcances para no mermar la lucha contra la ciberdelincuencia. De esta forma, sugiero que la única conducta excluida debe ser aquella perpetrada con dolo eventual, admitiendo tanto el dolo directo de primer grado como el dolo directo de segundo grado o dolo de consecuencias necesarias[492].

Una eventual reforma legislativa debe eliminar el término *deliberadamente* de su configuración.

Como ya se ha señalado, este delito excluye modalidades culposas, por ejemplo, si el agente accede a un sistema informático desconociendo su carácter restringido "ya que ese acceso fue facilitado, por ejemplo, por un empleado de la firma. También puede suceder que el que accede al sistema informático lo haga por indicación de un tercero, a quien se tiene por titular de ese sistema"[493].

A continuación, se presenta un caso diseñado por Alicia Gil Gil y Roberto Hernández Berlinches, quienes reflejan la ausencia de tipicidad subjetiva en el delito de acceso ilícito.

[Caso 59] Pedro llega a su puesto de trabajo por la mañana e intenta acceder al sistema de información de la empresa, pero obtiene un mensaje que le dice "usuario o clave incorrectos". Pensando que su mala memoria le ha hecho olvidar una vez más la clave tras la última modificación de esta siguiendo los protocolos de seguridad, utiliza la de su subordinado Antonio, quien se la dice sin sospechar nada, y mientras llama al servicio de apoyo

491 Pérez López, Jorge. *Delitos regulados en leyes penales especiales*. Lima: Gaceta Jurídica, 2019, p. 112.

492 Para Oré Sosa (*Delictum. Apuntes de derecho penal*, cit., p. 193) y Arévalo Minchola/Vega Aguilar (*Ciberdelitos. Análisis en el sistema penal*, cit., p. 263), el término *deliberado* circunscribe el castigo únicamente a conductas cometidas con dolo directo o de primer grado.

493 Aboso, *Derecho penal cibernético*, cit., p. 186.

informático para que le reestablezca la suya. En realidad, lo que ha sucedido es que una hora antes Pedro ha sido despedido de la empresa por un email, que todavía no ha abierto dado que para leerlo tenía que entrar a su ordenador, y en consecuencia se le han retirado todos los privilegios de acceso. Cuando Pedro accede al sistema con las claves de Antonio, ninguno de los dos conoce que el acceso no está autorizado. Por tanto, actúan sin dolo, no perpetran un acceso no autorizado intencionalmente[494].

5.7.2. Las modalidades de acceso ilícito

La vulneración de medidas de seguridad dividirá el tipo penal en dos modalidades diferentes: la primera será aquella en la que no son quebradas y que configurará una modalidad básica o inicial; la segunda se configurará cuando son transgredidas, estableciendo una modalidad agravada.

5.7.2.1. Sin vulneración de medidas de seguridad

El Informe Explicativo precisa que el medio de defensa más eficaz para prevenir accesos no autorizados es la utilización de medidas de seguridad. Sin embargo, aclara que es viable una respuesta de amplio alcance: "La prohibición penal en cuanto al acceso no autorizado puede brindar una protección adicional al sistema y a los datos propiamente dichos y en una primera etapa contra los peligros descritos más arriba"[495]. Así, desde diciembre del 2023, Perú eliminó la vulneración de medidas de seguridad como requisito para la configuración del tipo penal. Actualmente, el primer párrafo del artículo 2 LDI recoge dos modalidades: acceso (intrusismo) y exceso (abuso de confianza).

Considero que eliminar la vulneración de medidas de seguridad como requisito para la configuración del tipo penal es un adelantamiento excesivo de las barreras de protección penal[496].

494 Gil Gil/Hernández Berlinches, *Cibercriminalidad*, cit., p. 205.

495 Párrafo 45.

496 En el mismo sentido, Hernández Díaz, *Los accesos ilícitos a sistemas informáticos. Normativa internacional y regulación en el ordenamiento penal español*, cit., p. 293.

5.7.2.1.1. Acceso

Aunque parezca obvio, por un lado, este verbo exige un acceso no autorizado a un sistema informático ajeno. Por otro lado, en la investigación deberá comprobarse que el acceso, total o parcial, se produjo. Así, el investigador debe recordar que existe *malware* que le permite al ciberdelincuente obtener información de la víctima sin que haya accedido a su sistema[497]. En este último caso, no nos encontraremos frente al delito de acceso ilícito.

Ahora bien, por **acceso a todo o parte de un sistema informático** se entiende el ingreso o entrada a todo el sistema informático o a una sección independiente de este (*hardware* o sus componentes, BIOS o Basic Input-Output System/UEFI o Unified Extended Firmware Interface, sistema operativo, aplicaciones, etcétera). Es oportuno recordar que no importa la intención ulterior del sujeto activo, por ejemplo, obtener datos informáticos, pues se castiga el mero intrusismo o acceso ilícito.

El Informe Explicativo describe aún más esta conducta:

> El término "acceso" abarca la entrada a un sistema informático o a alguna parte del mismo (*hardware*, componentes, datos almacenados del sistema instalado, directorios, datos relativos al tráfico y datos relacionados al contenido). Sin embargo, no incluye el mero envío de un mensaje de correo electrónico o de un archivo a ese sistema. El término "acceso" incluye el ingreso a otro sistema informático, al que esté conectado a través de redes de telecomunicaciones públicas, o a un sistema informático que esté conectado a la misma red, como una LAN (red de área local) o a una Intranet (red interna) que opere en el seno de una organización. No tiene importancia el método de comunicación utilizado (por ej., desde lejos, incluidos los enlaces inalámbricos, o desde una corta distancia)[498].

Para el profesor Oré Sosa, acceder "supone asumir algún tipo de control sobre los procesos, datos o programas del sistema, ya sea que el acceso

497 En esta línea, Miró Llinares, *El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio*, cit., p. 55.

498 Council of Europe. *Convenio sobre la ciberdelincuencia. Informe explicativo*, Budapest, 23 de noviembre de 2001, párrafo 46. https://rm.coe.int/16802fa403.

se efectúe de manera directa o remota"[499]. Además, sobre el acceso total o parcial, precisa:

> Cabe el intrusismo parcial, pues ahí donde un sistema informático es compartido por distintas personas, a través de redes internas, existen ámbitos de privacidad individualizada cuya intromisión [...] constituye un acceso, si bien no a todo el sistema, a una parte de él[500].

Para que se configure este delito no se requiere el acceso total, pues se castiga, incluso, el acceso parcial. Así, existen sistemas informáticos que, una vez superada la medida de seguridad, el atacante accede a la totalidad. En cambio, existen otros sistemas que tienen secciones especialmente protegidas y a los cuales el atacante no puede acceder. De este modo, el ciberdelincuente habrá accedido al sistema, pero no a todo, ya que hay áreas protegidas a las que no puede ingresar. En este último caso, estaremos frente a un acceso parcial[501].

5.7.2.1.2. Exceso

El segundo párrafo del artículo 2 prevé la modalidad conocida como abuso de confianza, prevista también en la legislación de Argentina, Chile, Colombia y República Dominicana.

En este caso, el sujeto activo no vulnera las medidas de seguridad establecidas para impedir el acceso, pues ingresa con la autorización conferida por el usuario. Así, este ilícito se configura cuando **excede la autorización brindada**,

499 Oré Sosa, *Delictum. Apuntes de derecho penal*, cit., p. 191.

500 Oré Sosa, *Delictum. Apuntes de derecho penal*, cit., p. 192.

501 En otras palabras, imaginemos que el sistema es un edificio y que el delincuente obtuvo la llave de ingreso. Se desplaza por los cinco primeros pisos, pero al llegar al último, encuentra una puerta de acceso adicional que le impide subir a los pisos superiores. En esta línea: "[...] en el momento en que se tenga disponibilidad de la totalidad del sistema se habrá consumado el delito, pero en aquellos casos en los que se tenga disponibilidad sobre una parte del sistema existiendo una parte especialmente protegida sobre la que no se adquiere disponibilidad, entonces se tratará de un acceso parcial, consumándose la conducta igualmente por estar en condiciones el sujeto de acceder al contenido de la parte que ha logrado desproteger" (Montserrat Sánchez-Escribano, *El delito de acceso ilícito a un sistema informático: aspectos relativos a su regulación e interpretación*, cit., pp. 166 y s.).

es decir, realiza acciones que no fueron acordadas previamente -algunos autores denominan este supuesto como *el confidente necesario*[502]-.

Por ejemplo, si llevo mi laptop al servicio técnico por alguna falla específica y proporciono las claves de acceso para que realicen las pruebas correspondientes, el técnico cometerá este delito si, por ejemplo, accede a mis correos electrónicos o archivos personales, pues la autorización conferida no incluye tales permisos.

[Caso 60] El siguiente caso sucedió en España. Si bien se condujo bajo el artículo 197.2 *in fine*, norma que sanciona el acceso sin consentimiento a datos reservados de carácter personal atinentes a la salud registrados en soportes informáticos, en la legislación penal peruana puede ser subsumido como delito de acceso ilícito, en la modalidad de exceso de autorización.

Estibaliz, enfermera de atención primaria, entre el 11 de junio de 2014 y el 22 de marzo de 2016, accedió y visualizó desde un ordenador del hospital las historias clínicas de 16 compañeros. Así, sin permiso alguno, efectuó 60 accesos -registrados y probados en juicio-. La enfermera reconoció que sabía que solo se podía acceder por motivos sanitarios; sin embargo, admitió que lo hizo por motivos administrativos, alegando que conocía a los afectados.

Resulta interesante el enfoque adoptado por la Audiencia Provincial de León respecto a la figura del *insider*, ya que en ciertos supuestos se excede de la autorización otorgada en cuanto al acceso a la información y, en otros casos, directamente vulnera la confianza depositada en él, facilitando que terceros comprometan la seguridad informática de quien le concedió dicho acceso.

> Por ende, conductas claramente incursas en el art. 197.2 CP, con acceso a ficheros con datos personales, donde existe por otro lado, la posibilidad por responsables y encargados del tratamiento de un acceso lícito, pero que el sujeto activo sobrepasa; así esa casuística se refiere a un *intraneus* o *insider* en relación a los ficheros; es decir, persona que estando inicialmente autorizada para acceder a los datos y para realizar con ellos las operaciones previstas por el responsable del fichero de acuerdo con la ley, no lo está para otras conductas, o de personas que

502 Aboso, *Derecho penal cibernético*, cit., p. 186.

> realizan consultas a las bases de datos de las que obtienen información mediante el empleo de su clave personal que permitía entrar a las mismas, si bien por la asignación de funciones no le correspondieran tareas en esa específica área, en ese nivel, o en relación a esos concretos datos consultados[503].

La doctrina sitúa como fuente legislativa de esta modalidad el ordenamiento legislativo de Estados Unidos, diferenciándolo así de ordenamientos europeos que sancionan el mantenerse en un sistema informático en contra de quien tiene el legítimo derecho a excluirlo.

> En el supuesto conocido en Estados Unidos de América como exceso en la autorización, el sujeto activo ostenta un título jurídico que le permite acceder a la totalidad del sistema, pero con unas facultades concretas. En lugar de criminalizar este supuesto con base en la formulación de una nueva modalidad típica, la Sección 1030 del Código Penal Federal de los Estados Unidos de América hace descansar estructuralmente la tipicidad de la acción en el consentimiento. Así, la acción siempre es la misma: el acceso, pero la responsabilidad penal se activa tanto cuando el sujeto accede al sistema en ausencia de consentimiento, esto es, sin autorización (*without authorization*), como cuando, gozando del mismo, existe un exceso en la autorización concedida (*exceeding authorized access*).
>
> La literatura norteamericana vincula directamente la acción con el término de *insiders* (por contraposición al acceso sin autorización que sería cometida por *outsiders*), es decir, aquellos sujetos que ostentan algún género de facultad de acceso sobre el sistema informático y la información. Aunque esta conducta tiene su sede original en el seno de una relación laboral, también se plantea esta conducta en el contexto de las relaciones contractuales de carácter civil[504].

503 SAP LE 528/2021. Sentencia N.º 94/2021 del 4 de marzo de 2021, emitida por la Audiencia Provincial de León, Sección N.º 3. Ponente: María del Mar Gutiérrez Puente.

504 Montserrat Sánchez-Escribano, *El delito de acceso ilícito a un sistema informático: aspectos relativos a su regulación e interpretación*, cit., pp. 181 y s.

En este punto es importante advertir que, en la industria de la ciberseguridad, existen los denominados *white hats*, *hackers* de sombreros blancos o *hackers* éticos, quienes son contratados por las empresas para identificar vulnerabilidades y deficiencias y, de este modo, recomendar sus mejoras. En algunas ocasiones, no tienen contratos, pero participan en programas de *bug bounty*, es decir, las empresas ofrecen recompensas monetarias y reconocimientos a quienes encuentren vulnerabilidades en sistemas, sitios y redes[505].

[Caso 61] En el 2014, Telegram activó un programa de recompensas por errores de su plataforma. Los premios oscilan entre 100 y 100 000 dólares americanos, según la gravedad del problema. Es importante señalar que, en la web, Telegram precisa que no emprenderá acciones legales contra nadie que investigue y divulgue vulnerabilidades de manera responsable de acuerdo con sus reglas. Así, reglas y principios que rigen esta actividad son los siguientes:

- Sus pruebas no pueden violar ninguna ley, interrumpir los servicios de Telegram ni afectar negativamente a otros usuarios de ninguna manera.
- Las vulnerabilidades que se revelan al público o a terceros antes de que se solucionen no son elegibles para nuestro programa de recompensas por errores. Esto incluye a los agentes de vulnerabilidades.
- Está estrictamente prohibido intentar obtener acceso físico a cualquier equipo de Telegram.
- Si es elegible para un premio, usted será responsable de los impuestos y tarifas según su país de residencia.
- Este programa de recompensas está enfocado en la seguridad y, por lo tanto, no cubre problemas de denegación de servicio o equilibrio de carga que resulten de spam, ataques de fuerza bruta, ataques DDoS coordinados, etc. En consecuencia, no se le permite realizar ninguna acción de este tipo en nuestros servicios[506].

505 Reale, Julián M. "Importancia de la instrumentalización jurídica de la *vulnerability assessment* y la etapa de explotación de vulnerabilidades para evitar su criminalización". En: Salt, Marcos G. (Dir). *@UBACibercrimen | 1*. Buenos Aires: Ad-Hoc, 2022, p. 52.

506 Disponible en: https://core.telegram.org/bug-bounty

Si bien el *ethical hacking* no necesita ninguna formalidad, pues la autorización y las instrucciones podrían ser brindadas de forma verbal, generalmente se verá reflejada en un contrato de servicios de seguridad informática[507]. Dicho contrato será útil para conocer las facultades del experto y, además, probar si se actuó o no en el marco de la autorización. Como se puede apreciar, el contrato de servicios o los términos y condiciones del *bug bounty* serán sumamente relevantes para conocer o probar si nos encontramos frente a una actuación lícita o si, al haberse excedido la autorización, la conducta configura la modalidad de acceso ilícito aquí estudiada.

5.7.2.2. Con vulneración de medidas de seguridad

El segundo párrafo del artículo 2 LDI establece una segunda modalidad: el acceso ilegal en el que se **vulneran las medidas de seguridad establecidas para impedirlo**. Una defensa, salvaguarda o medida de seguridad es cualquier medio empleado para eliminar o reducir un riesgo. Su objetivo es reducir las vulnerabilidades de los activos, la probabilidad de ocurrencia de las amenazas y/o el nivel de impacto en la organización[508].

Las medidas de seguridad están asociadas con la autenticación, esto es, "el proceso mediante el cual se verifica que alguien es quien dice ser"[509]. Podríamos dividir las medidas de seguridad en tres grandes grupos: Algo que uno conoce (contraseñas), algo que uno tiene (*token* físico o tarjeta) o algo que uno es (biometría):

507 Palazzi, "El delito de acceso ilegítimo a un sistema informático", cit., pp. 47 y s.

508 Gómez Vieites, *Enciclopedia de la Seguridad Informática*, cit., p. 68.

509 Caballero/Cilleros Serrano, *El libro del hacker. Edición 2022*, cit., p. 418.

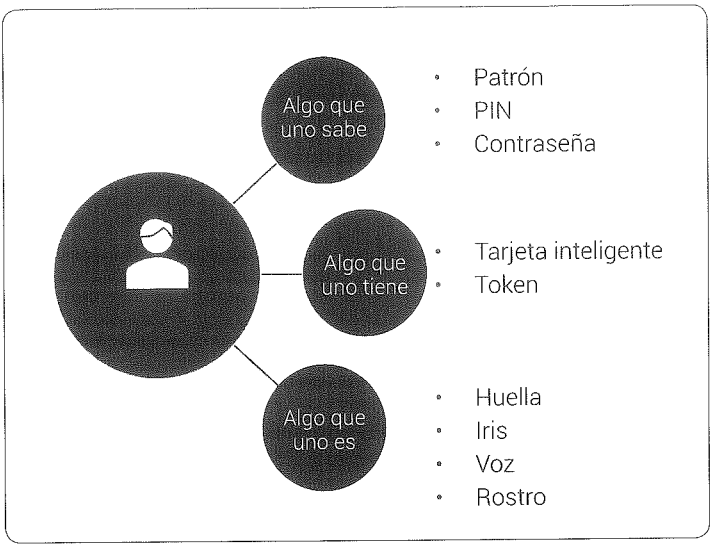


Diagrama 8. Elementos de seguridad que puede adoptar un usuario. Adaptación[510].

Para que se configure la modalidad bajo estudio, acceso mediante quebrantamiento de medidas de seguridad, el usuario debería haber implementado por lo menos un factor de autenticación -pues, en la práctica, existen factores dobles o múltiples factores o MFA, por sus siglas en inglés-[511].

A continuación, enumeraremos algunas medidas de seguridad o métodos de autenticación que el usuario podría adoptar[512]:

a) **Secreto memorizado.** Su uso es el más extendido. En estos casos, el usuario debe recordar una serie de números (PIN), una combinación de caracteres (contraseña) o unir puntos en un orden

510 El gráfico es una adaptación de la figura elaborada por *Ibid.*, p. 419.

511 Si el usuario protege el acceso a su red social con una contraseña, estaremos frente a un factor único de autenticación. Si, además, debe colocar el número de verificación que recibe en su dispositivo móvil después de ingresar la contraseña, estaremos frente a un factor doble de autenticación. Obviamente, si se agregan más medidas de seguridad, nos encontraremos frente a un *Multifactor Authentication*.

512 Los métodos de autenticación descritos entre los literales a y e, han sido tomados o adaptados de: Caballero/Cilleros Serrano, *El libro del hacker. Edición 2022*, cit., pp. 420-425. El literal f ha sido desarrollado, a partir de: Instituto Nacional de Ciberseguridad. *Bloqueo de dispositivos: patrón, contraseña, PIN, código y biometría.* https://www.incibe.es/ciudadania/tematicas/dispositivos-moviles/bloqueo-dispositivos

específico (patrón). Para garantizar la confidencialidad, este *secreto* debe viajar empleando un protocolo criptográfico.

b) **Secreto basado en consultas.** El usuario almacena un conjunto de claves secretas en un soporte físico -por ejemplo, en una tarjeta de coordenadas- o electrónico. Por lo general, son grupos de números ordenados en filas y columnas. Para acceder, el sistema solicitará una o más líneas de las celdas.

c) **One Time Password (OTP).** Es una clave que puede utilizarse por una sola vez y durante un tiempo limitado. Las OTP se generan criptográficamente. Un ejemplo es la llave *token* que entregan los bancos para realizar operaciones comerciales.

d) **Autenticación por fuera de banda (OOB).** En este caso, se emplean códigos de un solo uso compartidos a través de un dispositivo fuera de banda, con el cual se introduce un segundo factor de autenticación. El usuario deberá registrar previamente un dispositivo, el cual recibirá el código de verificación. Por ejemplo, el usuario registra su celular para recibir únicamente en ese dispositivo el SMS que será empleado para verificar su identidad.

e) **Dispositivos criptográficos.** Tipo de dispositivos físicos que realizan operaciones criptográficas para la generación de claves, públicas y privadas, garantizando que no puedan ser exportadas a otros soportes. Los *token* criptográficos pueden presentarse como USB o como tarjetas inteligentes (*smart card*).

f) **Biometría.** Medida de seguridad que emplea las características físicas del usuario, por ejemplo, reconocimiento facial, huella dactilar y reconocimiento de voz, reconocimiento de iris.

Las medidas de seguridad pueden ser activas o pasivas. Las primeras buscan anular o reducir el riesgo de la amenaza de manera preventiva (antes del incidente) o a través de su detección (durante el incidente). Las segundas buscan reducir el impacto cuando se produce el incidente, por lo que también se les conoce como *medidas de corrección*. El segundo párrafo del artículo 2 LDI se refiere a la trasgresión de las medidas de seguridad activas de prevención, como la autenticación de usuarios, el control de acceso a los ficheros, el cifrado de datos sensibles, entre otros.

Si bien las medidas de seguridad pueden ser físicas o lógicas[513], considero que este tipo penal sanciona solo la vulneración de las segundas[514]. Así, por ejemplo, si dejo mi computadora encendida y sin ningún tipo de medida de seguridad lógica, pero cierro la puerta de mi oficina para mantener alejados a terceros (seguridad física), no responderá, bajo el segundo párrafo del artículo 2 LDI, quien irrumpe con un duplicado de la llave o fuerza la chapa de ingreso y logra ver el contenido de mi información. Llego a esta conclusión, tomando en consideración el artículo 1 de la citada norma, pues precisa que nuestra legislación especial busca sancionar las conductas cometidas a través de las TICs[515]:

513 "Las medidas de seguridad pueden dividirse en "medios de carácter lógico", los cuales están integrados por aplicaciones de tipo *software* y "medios de carácter físico" entre los que se pueden distinguir los instrumentos *hardware* y mecanismos de tipo organizativo". Citando la tesis doctoral de María Isabel Sánchez-Escribano Montserrat: Rodríguez Rocha, "El delito de acceso ilícito a los sistemas informáticos. Análisis del tipo penal y el rol de la cooperación judicial internacional", cit., p. 342.

514 En sentido contrario: "El tipo al no poseer detalles del carácter o naturaleza de las medidas de seguridad, como bien se señala estas deben interpretarse ampliamente como cualquier tipo de medida dirigido a proteger datos y programas con un mínimum de eficacia y estas (medidas) muy bien pueden ser físicas o lógicas" (García León, "Análisis del tipo de acceso ilícito. Bien jurídico, tipicidad objetiva y subjetiva, autoría y participación, y su distinción con el delito de atentado a la integridad de datos y sistemas informáticos", cit., p. 370).

515 Al analizar la doctrina española, encuentro que cierto sector considera que la medida de seguridad vulnerada puede ser tanto lógica como física. Sin embargo, considero que se arriba a esta conclusión porque el delito se ubica en el CP y no en una norma especial, en un capítulo que protege la intimidad y no la confidencialidad informática, y, finalmente, porque adolecen de una norma que delimite el ámbito de protección -como el art. 1 LDI-. "No obstante, como ya hemos mencionado, a pesar de que lo característico del *hacking* es el acceso a los sistemas de información, o parte de los mismos, neutralizando las medidas de seguridad mediante conductas telemáticas, nos encontramos ante un delito de medios indeterminados y, por tanto, la descripción típica no excluye la sanción de conductas de acceso de carácter puramente físico. Así, cabría, por ejemplo, sancionar a quien accede a un ordenador guardado por su legítimo propietario dentro de un cajón cerrado con llave, aunque tras forzar el cajón solo tenga que encender el dispositivo para así acceder a este sistema de información" (Hernández Díaz, Leyre. "La regulación penal del *hacking* blanco: el modelo del Código Penal español". En: Caro Coria, Carlos Dino y Luis Reyna Alfaro (dirs.). *Ciberseguridad, cibercrimen y nuevas tecnologías. Riesgos y respuestas jurídicas*. Ciudad de México: Derecho Global Editores, 2022, p. 291).

> **Art. 1 LDI.-** La presente Ley tiene por objeto prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, **cometidas mediante la utilización de tecnologías de la información o de la comunicación**, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia [El resaltado es mío].

El delito de acceso ilícito, en otras latitudes, no se encuentra ubicado en un capítulo específico que reconozca la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos como bien jurídico protegido. Es más, en muchas ocasiones tampoco está recogido en una norma especial como la LDI. Por esta razón, otras legislaciones sí permiten comprender las herramientas físicas como medidas de seguridad[516]. Insisto, la ubicación y el artículo 1 LDI restringen esta interpretación en el caso peruano.

Ahora bien, la vulneración de las medidas de seguridad se configura, incluso si un usuario legítimo le proporciona la clave de acceso a alguien que no debería tener. Esto se conoce como *el empleado infiel*[517].

Generalmente pensamos que vulnerar una medida de seguridad es ingresar una contraseña o un código complejo o sofisticado, pero no necesariamente es así. Incluso si el usuario emplea medidas de seguridad que fácilmente pueden ser adivinadas u obtenidas, el tipo penal igual se configurará[518].

En diciembre del 2024, la empresa de ciberseguridad NordPass publicó la lista de contraseñas más utilizadas a nivel mundial y el tiempo en el que podrían ser descifradas. Insisto, incluso los usuarios que configuren sus sistemas con estas contraseñas se encuentran protegidos frente al intrusismo informático -otra cosa será, el nivel de vulnerabilidad al que se encuentran expuestos-:

---

516 Sobre la problemática en torno a las medidas de seguridad física, ver: Hernández Díaz, "La regulación penal del *hacking* blanco: el modelo del Código Penal español", cit., pp. 293 a 296.

517 Aboso, *Derecho penal cibernético*, cit., p. 186.

518 "En cuanto a las características que tendrán estas medidas de seguridad, la doctrina viene reclamando que deben ser las que normalmente utilizaría un usuario medio, sin exigirse que sean especialmente sofisticadas o de difícil uso para la mayoría de la población usuaria de los sistemas de información" (Hernández Díaz, "La regulación penal del *hacking* blanco: el modelo del Código Penal español", cit., p. 296).

Posición	Contraseña	Tiempo para descifrarlo	Frecuencia de uso
1	123456	< 1 segundo	3 018 050
2	123456789	< 1 segundo	1 625 135
3	12345678	< 1 segundo	884 740
4	password	< 1 segundo	692 151
5	qwerty123	< 1 segundo	642 638
6	qwerty1	< 1 segundo	583 630
7	111111	< 1 segundo	459 730
8	12345	< 1 segundo	395 573
9	secret	< 1 segundo	363 491
10	123123	< 1 segundo	351 576
11	1234567890	< 1 segundo	324 349
12	1234567890	< 1 segundo	324 349
13	1234567	< 1 segundo	307 719
14	000000	< 1 segundo	250 043
15	qwerty	< 1 segundo	244 879
16	abc123	< 1 segundo	217 230
17	password1	< 1 segundo	211 932
18	iloveyou	< 1 segundo	197 880
19	11111111	< 1 segundo	195 237
20	dragon	< 1 segundo	144 670

Cuadro 17. Las 20 contraseñas más usuales, empleadas a nivel mundial en el 2024[519].

Si le sorprende la facilidad y rapidez de los ciberdelincuentes para descifrar sus claves de seguridad, debe saber que, hoy en día, utilizando el poder computacional almacenado en la nube y herramientas como Cloud-Cracker, "puedes probar trescientos millones de variaciones de tu contraseña potencial en unos veinte minutos por un coste de unos 17 dólares. Ello implica que cualquiera podría alquilar servicios de computación en la nube de Amazon para descifrar la clave de encriptación normal que protege la mayoría de las redes Wi-Fi en menos de seis minutos, todo ello por la irrisoria suma de 1,68 dólares en tiempo de alquiler"[520].

Ahora bien, estimado lector, ¿qué pasaría si, por un error de configuración, sin ingresar un solo dígito, pero apretando la tecla «Enter», se accede al sistema? ¿Estaríamos frente a un acceso ilícito con el quebrantamiento de

519 Nordpass. *Las top 200 contraseñas más comunes.* https://nordpass.com/es/most-common-passwords-list/

520 Goodman, Marc. *Los delitos del futuro. Todo está conectado. Todos somos vulnerables. ¿Qué podemos hacer al respecto?* Barcelona: Ariel, 2019, p. 329.

medidas de seguridad? A continuación, veremos un caso tan famoso como problemático.

[Caso 62] En el 2022, el ciudadano británico Gary McKinnon se encontraba obsesionado con el gobierno de los Estados Unidos, pues pensaba que ocultaba información sobre la vida fuera de nuestro planeta, es decir, sobre los extraterrestres. Así, luego de correr un *script* (secuencia de comandos básica), advierte que algunas cuentas de la NASA no exigían colocar una contraseña, solo se debía digitar la tecla «Enter» para acceder a su información. Si colocaban cualquier otra combinación, el sistema impedía el acceso.

De este modo, McKinnon logró acceder a los sistemas durante dos años. La fiscalía pidió hasta 70 años de prisión, argumentando que accedió a 97 computadoras, obtuvo 950 contraseñas y eliminó 1300 cuentas de internet. Según el gobierno de Estados Unidos, esto generó daños ascendentes a 800 000 dólares americanos, catalogando el incidente como el mayor ataque a sistemas informáticos militares del país.

En el 2012, la ministra del Interior del Reino Unido rechazó la solicitud de extradición requerida por Estados Unidos, tomando en consideración la condición médica de Gary: padecía del síndrome de Asperger y sufría de depresión, lo que se hubiese agravado tomando en consideración la sanción a imponer de aceptarse el pedido:

> El señor McKinnon está acusado de delitos graves. Pero tampoco hay duda de que está gravemente enfermo. Tiene síndrome de Asperger, y sufre de depresión. La cuestión jurídica ante mí ahora es si el alcance de esa enfermedad es suficiente para impedir la extradición.
>
> Después de una cuidadosa consideración de todo el material relevante, he llegado a la conclusión de que la extradición del señor McKinnon daría lugar a riesgo tan alto de que termine su vida que la decisión de extraditar sería incompatible con los derechos humanos del señor McKinnon[521].

521 "Una brecha en la NASA y supuesta evidencia de "vida extraterrestre", en welivesecurity, 9 de diciembre de 2015. https://www.welivesecurity.com/la-es/2015/12/09/brecha-nasa-vida-extraterrestre/; "Hacker británico cerca de la extradición", en *Bbc Mundo.*, 31 de julio de 2009. https://www.bbc.com/mundo/internacional/2009/07/090731_

Desde mi punto de vista, sí existió un quebrantamiento de las medidas de seguridad, aunque no hubiese tenido que ingresar un solo dígito o carácter. De este modo, cuando el sistema emite un mensaje y solicita una clave, ya podemos afirmar que existe una medida que superar. Al analizar la medida de seguridad adoptada, es irrelevante si es o no sólida, compleja o robusta e, incluso, si ha sido establecida por el instalador del sistema, el administrador o el propio usuario -lo importante es que se encuentre operativa para quien se encuentra legitimado para utilizarla-[522].

Ahora bien, las **brechas de seguridad**[523] son cada vez más usuales. Muchas veces, en vez de crear un usuario y generar una contraseña, asociamos una aplicación o membresía con nuestro correo electrónico o red social favorita. Al hacerlo, podríamos exponer nuestros datos e información si es que un actor de amenazas ataca la aplicación o el servicio en el que nos hemos registrado y, de este modo, accede a sus registros. Esto no significa que he sido *hackeado*, sino que el ciberdelincuente accedió a la base de datos de un sistema que almacena mi información y la de miles o millones de usuarios.

Actualmente, existen servicios *online* que permiten identificar las brechas de seguridad y si nuestra información se ha visto comprometida. **Have I been pwned** es una página web que permite comprobar qué datos nuestros -contraseñas, por ejemplo- podrían haberse filtrado en un ciberataque.

---

hacker_lh; Eve, Martin Paul. *Una historia de las contr43eñ4s*. Buenos Aires: Godot, 2023, pp. 13 y 47.

522 Gil Gil/Hernández Berlinches, *Cibercriminalidad,* cit., p. 203.

523 "Una brecha de seguridad es cualquier incidente en el que la confidencialidad, integridad o disponibilidad de los datos de una organización es comprometida debido al acceso no autorizado, divulgación, alteración o destrucción de la información. Este tipo de incidente puede abarcar múltiples formas de ataques, desde el robo de credenciales hasta la explotación de vulnerabilidades en sistemas, e incluso filtraciones causadas por errores humanos o fallos en los procesos internos". Instituto Nacional de Ciberseguridad. *¿Cómo manejar una brecha de seguridad. Pasos críticos: desde la contención hasta la recuperación y comunicación con los afectados?,* p. 5. https://www.incibe.es/sites/default/files/Emprendimiento/Guía_manejar_brecha_seguridad/Guía_Cómo%20manejar%20una%20brecha%20de%20seguridad.pdf

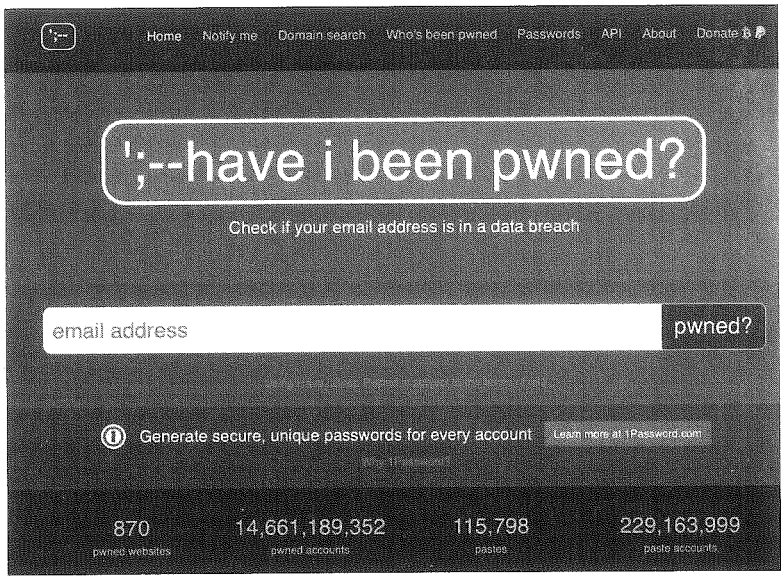


Imagen 12. Página principal del proyecto *Have I been pwned?*[524].

Si el lector ingresa a la página web y coloca su correo electrónico o número celular (anteponiendo el + y el código del país), podrá conocer si se encuentra en alguna filtración. Por ejemplo, al colocar un correo electrónico pude identificar que este se encontraba asociado a 9 brechas de seguridad, una de ellas, relacionada a Telegram:

> **Combolists Posted to Telegram:** In May 2024, 2B rows of data with 361M unique email addresses were collated from malicious Telegram channels. The data contained 122GB across 1.7k files with email addresses, usernames, passwords and in many cases, the website they were entered into. The data appears to have been sourced from a combination of existing combolists and info stealer malware.
>
> Compromised data: Email addresses, Passwords, Usernames

A veces se piensa que el acceso ilícito con el quebrantamiento de medidas de seguridad exige herramientas sofisticadas y no es así. Recuerdo alguna diligencia que tuve en una unidad policial especializada en la que el oficial a cargo tenía anotado en un *post it* su usuario y contraseña. Bastaba tomar

524 Disponible en: https://haveibeenpwned.com

una fotografía o anotarlo para ingresar ilegalmente, claro está, a su sistema informático.

Ahora bien, imagínese que el lector es un empresario, un juez o un fiscal y su competencia o un investigado quiere acceder a sus correos electrónicos con la finalidad de obtener información comprometedora. Averiguar el correo institucional o personal no es una labor difícil. Si el agente lo obtiene, podría indagar si dicho correo estuvo comprometido en una brecha de seguridad (con la página web antes mencionada) y, luego, comprar esos datos en el mercado negro de la *dark web*[525]. Por eso es muy importante tener contraseñas robustas y, con cierta frecuencia, cambiar o actualizarlas.

5.7.2.2.1. Acceso con vulneración de medidas de seguridad

El segundo párrafo del artículo 2 LDI solo castiga el acceso ilegal con vulneración de medidas de seguridad. Esto es obvio, pues el exceso -como se ha dicho- se conoce como abuso de confianza. De este modo, en el exceso no habrá dicha vulneración, pues no es necesaria, ya que el agente ingresa sin dificultad, precisamente, por la confianza que el titular del sistema ha depositado en él.

El acceso puede ser físico o remoto[526] -lo que no debe confundirse con el tipo de medida de seguridad que protege el sistema-. En este caso, se estudia la ubicación del sujeto activo frente al sistema informático protegido:

a. Acceso físico. Supone la intervención física, directa o material del sistema informático por parte del sujeto activo, que se introduce

525 El portal web especializado en ciberseguridad Xataka informa que en la dark web se pueden comprar datos de tarjetas de crédito españolas con CCV por 34 euros aproximadamente. Además, advierten que "nuestros datos pueden acabar en manos de actores maliciosos incluso si nuestro ecosistema digital no se ha visto involucrado en un incidente directamente. También existe la posibilidad de que algunos de los servicios en los que confiamos sufran una brecha de seguridad que expongan nuestros datos, que puede ser información personal como nuestros nombre y apellido, pero también nombres de usuario, contraseñas, datos bancarios y más". MÁRQUEZ, Javier. *Tu DNI, a la venta por 15 euros en la dark web: cuánto valen nuestros datos robados en el mercado negro de Internet*, publicado el 4 de enero de 2025. https://www.xataka.com/seguridad/tu-dni-a-venta-15-euros-deep-web-cuanto-valen-nuestros-datos-robados-mercado-negro-internet

526 MONTSERRAT SÁNCHEZ-ESCRIBANO, *El delito de acceso ilícito a un sistema informático: aspectos relativos a su regulación e interpretación*, cit., p. 165.

en él desde el mismo lugar donde se encuentra utilizando únicamente sus propios elementos de *hardware* y *software*.

b. Acceso lógico o remoto. Consiste en la introducción indirecta o virtual en el sistema informático accedido, utilizando otro sistema informático o cualquier otro dispositivo electrónico o telemático que, mediante *software*, permita el intercambio de información para introducirse en el sistema informático objeto de acceso, lo que exige que ambos sistemas estén conectados o bien a una red de área global, como Internet, o bien a una red de área local.

En Perú, se sanciona tanto el acceso físico o directo como el acceso remoto[527].

A continuación, siguiendo a María Ángeles Caballero y Diego Cilleros Serrano[528], analizaremos 15 técnicas y subtécnicas que emplean los ciberdelincuentes para acceder a los sistemas informáticos. Sin embargo, veremos que algunos ataques vistos de forma aislada configurarían el delito de interceptación de datos informáticos -por ejemplo, el ataque del hombre del medio o MITM-.

a. **Fuerza bruta**. El atacante ingresa diversas combinaciones de claves, esperando que alguna de ellas le permita acceder al sistema. Si bien puede realizarse de forma manual, también existen *softwares* que cumplen dicha finalidad. Entre las modalidades de ataque de fuerza bruta[529], tenemos las siguientes:

---

527 Recordemos que el Convenio de Budapest señaló que los diferentes estados miembros podían elegir si adicionaban como elemento del tipo, la necesidad de que el ataque sea remoto: "Las Partes podrán exigir que el delito se cometa [...] en relación con un sistema informático conectado a otro sistema informático". Perú no lo agregó en su estructura típica.

528 Para explicar estos quince tipos de ataque, he tomado como eje central de referencia: Caballero/Cilleros Serrano, *El libro del hacker. Edición 2022*, cit., pp. 427-431. No está demás decir que recomiendo la lectura de la publicación de los autores en referencia, pues describen con mucho más detalle y claridad los diversos ataques aquí estudiados. De otro lado, para la descripción de los ataques, se complementó con: Instituto Nacional de Ciberseguridad. *Con estos ataques nos roban las contraseñas, ¡aprende a evitarlos!* https://www.incibe.es/empresas/blog/estos-ataques-nos-roban-las-contrasenas-aprende-evitarlos

529 "Brute force (fuerza bruta). Un enfoque un tanto no técnico para obtener una contraseña en la que se intentan todas las combinaciones posibles de opciones hasta

- **Ataque de diccionario**. El atacante utiliza palabras o frases comunes, en lugar de combinaciones aleatorias. Más adelante, se enlistan 20 contraseñas comunes y el tiempo que a un *software* le tomaría descifrarlas -como se verá, en todos los casos es menos de un segundo-.
- **Relleno de credenciales** (*credential stuffing/credential reuse*). Se utilizan credenciales obtenidas en brechas de seguridad. Como muchos usuarios reutilizan la misma credencial en diferentes sistemas, basta que el ciberdelincuente obtenga una de ellas para aprovecharla.
- **Ataque de pulverización de contraseñas** (*password spraying*). Se selecciona un número limitado de usuarios y de credenciales para probarlas en ellas. Por ejemplo, se podrían seleccionar las cuentas de trabajadores de una empresa o de una institución pública y probar determinadas contraseñas obtenidas en una brecha de seguridad o, a través de ataques de ingeniería social. Esta técnica es empleada para minimizar el riesgo de bloqueo o que los intentos de intrusión alerten a los sistemas de seguridad.

b. **Almacenes de contraseñas.** Los ciberdelincuentes se dirigen contra lugares que resguardan o custodian credenciales de usuarios, por ejemplo, algún lugar del sistema o aplicaciones que las almacenan.

   Hoy en día, existen muchas aplicaciones que brindan el servicio de almacenamiento de contraseñas, entre las principales se encuentran LastPass, 1Password, Dashlane, Keppass, Bitwarden, RoboForm, True Key, Sticky Password, Enpass y NordPass. Imaginemos que estas *apps* son una especie de bóveda y las credenciales que hay en ellas son el botín que el agresor espera obtener.

c. **Explotación para acceso a credenciales.** Conocida como Pass-The-Ticket, el atacante obtiene *tickets* Kerberos mediante el robo, compra o reutilización, que le permiten acceder al sistema. Pueden ser Ticket Granting Ticket (TGT) o Ticket de Servicio (TGS).

---

que se obtiene el valor correcto" (Angulo Aguirre, *Hacking & cracking – Redes inalámbricas Wi-Fi*, cit., p. 227).

Los TGT son tickets de autenticación principal y permiten solicitar TGS. Estos últimos permiten acceder a servicios específicos del sistema, por ejemplo, un servidor de archivos o una base de datos.

d. **Autenticación forzada**. Los atacantes buscan obtener las credenciales del usuario, engañándolo. De este modo, cuando el usuario ingresa su clave, es retransmitida al atacante. Este tipo de ataques suelen emplear programas como el SMB Relay y el SNB Relay 2.

e. ***Forge web credentials***. El atacante falsifica los materiales de credenciales o *credential materials* que se utilizan para acceder a aplicaciones web o servicios de internet. Dada la sofisticación del ataque, requiere valores secretos como contraseñas, claves privadas o valores de la semilla criptográfica.

f. **Capturar la entrada.** El atacante busca capturar las contraseñas de acceso, por ejemplo, a páginas web visitadas por el usuario. Es común emplear *keyloggers* -"programa malicioso que registra y rastrea todas las pulsaciones en un dispositivo infectado"[530]- o páginas falsas que recopilan los datos de acceso de los usuarios.

   Sobre esta técnica, es importante diferenciar dos momentos: la captura de entrada para obtener las credenciales de acceso y el empleo de estas para acceder al sistema. La primera conducta configurará el delito de interceptación ilegal de datos, mientras que la segunda, el delito de acceso ilícito.

g. **Man-in-the-Middle**. En este ciberataque, estudiado en el primer capítulo, el atacante se interpone entre el usuario y el servidor para interceptar, modificar o sustraer los datos -en el caso que nos ocupa, credenciales de autenticación- sin que las partes se den cuenta.

   Imagine, estimado lector, que va a un restaurante a almorzar. El mesero toma su pedido en un papel y lo deja en la cocina. Un curioso podría leer la nota, copiarla o cambiarla -pues sabe que es alérgico a los langostinos y tacha esa observación-. Usted sería el usuario; su pedido, los datos informáticos -entre ellos, sus contra-

530 Instituto Nacional de Ciberseguridad. *Keylogger*. https://www.incibe.es/node/494000

señas-; el mesero, el *router* o servidor; y, finalmente, el curioso, el hombre del medio o atacante MITM.

h. **Modificar el proceso de autenticación.** Los ciberatacantes modifican el proceso de autenticación para acceder a las credenciales de los usuarios y, de este modo, lograr el acceso ilegal. Caballero y Cilleros detallan algunos tipos de ataque: autenticación de controladores de dominio, filtrado de contraseñas por DLL, *pluggable authentication modules*, autenticación de dispositivos de red.

i. **Escucha de red (*network sniffing*).** El ciberdelincuente intercepta, captura y analiza el tráfico de datos en una red. De este modo, puede ver las credenciales de usuario -en caso no estén cifradas-, las cookies de sesión, mensajes, etc.

   Como el lector habrá advertido, esta es una modalidad de interceptación de datos informáticos. Sin embargo, recordemos que estos sirven para identificar cómo se obtienen o utilizan las medidas de seguridad de los usuarios para acceder a sus sistemas.

j. **Volcado de credenciales del sistema operativo** (OS *credential dumping*). En esta técnica, el ciberdelincuente busca obtener los datos de usuario y las claves almacenadas en un sistema operativo, generalmente en texto cifrado o formato *hash*.

   Imaginemos un hotel de lujo. Cada huésped tiene una llave electrónica que le permite ingresar únicamente a su habitación. El hotel guarda una base de datos de todas las llaves electrónicas, pero, además, el gerente y ciertos empleados tienen una llave maestra con la que pueden entrar a cualquier habitación. ¿Qué preferiría un ladrón para maximizar sus fechorías y minimizar el riesgo? ¿Intentar robar una a una cada llave, hacer una copia de toda la base de datos u obtener la llave maestra?

   En la modalidad de ataque que estamos viendo, el ciberdelincuente razona de la misma manera. En vez de ir por cada cuenta de usuario (llave de cada huésped del hotel), puede ir por la base que almacena todas las llaves electrónicas (aunque podría toparse con llaves encriptadas que no podría descifrar) o por la llave maestra (*hash* del administrador de dominio) que le abrirá todas las puertas.

k. **Robar el *token* de acceso de la aplicación**. Tal y como vimos líneas arriba, los *token* están vinculados a las medidas de seguridad OTP (*one time password*). En estos casos, el ciberdelincuente busca acceder a estas credenciales a través de ataques de MITM, *malwares* o troyanos, *phishing*, vulnerabilidades XSS y, de este modo, como fácilmente se puede advertir, el objetivo del ciberdelincuente será obtener los códigos generados por el *token* y acceder al sistema deseado.

l. **Robar o falsificar los *tokens* de kerberos**. Este tipo de ataque, de forma general, lo vimos líneas atrás bajo el nombre *explotación para acceso a credenciales*. Es tal su relevancia que exige un tratamiento independiente.

   Kerberos es un protocolo de autenticación utilizado en los sistemas Windows Active Directory. Para comprender su funcionamiento, podríamos emplear una analogía: imagina que necesitas ingresar a un edificio con altas defensas y medidas de seguridad. Sin Kerberos, al ingresar al edificio, y cada vez que desees acceder a un ambiente, deberías identificarte una y otra vez -lo cual sería sumamente tedioso. Gracias a Kerberos, solo debes identificarte al ingresar al edificio, pues en recepción te otorgarán un *ticket* o *pase especial* (TGT). Así, cada vez que deseas ingresar a un área, en vez de volver a identificarte, solo muestras el *ticket* y te darán otro (TGS) que te permitirá acceder temporalmente.

   Entre los ataques que podemos identificar, entre otros, tenemos: **golden ticket** (el ciberdelincuente obtiene una llave maestra que le permite generar *tickets* kerberos por tiempo ilimitado), **silver tickets** (el atacante compromete credenciales de servicios específicos), **kerberoasting** (el atacante solicita *tickets* TGS de cuentas privilegiadas y los *crackea offline* para obtener contraseñas en texto claro).

m. **Robar las *cookies* de sesión**. Las *cookies* son archivos que los sitios web almacenan en el navegador del usuario para mantenerlo autenticado sin pedir la contraseña en cada acción realizada. Es una práctica común en páginas web de los sistemas financieros y en las redes sociales.

   En estos casos, el ciberdelincuente busca apropiarse de esas *cookies* para poder navegar en el sistema sin pedir autorizaciones. Existen

diferentes formas de conseguirlo, por ejemplo, a través de ataques de MITM, *malwares* y troyanos, ataques de ingeniería social, extensiones maliciosas, entre otras.

n. **Interceptar el segundo factor de autenticación**. Como hemos visto, es recomendable contar con un segundo factor de autenticación para proteger los sistemas informáticos. Los ciberdelincuentes lo saben y buscan obtener el dominio de estos. Así, por ejemplo, podrían sustraer físicamente el *token* o la tarjeta inteligente, aplicar técnicas de ingeniería social para conocer la clave que es recibida por la víctima o utilizar *keyloggers* que permitan interceptar los dígitos o caracteres.

o. **Credenciales inseguras**. Los ciberdelincuentes podrían atacar y buscar sistemas comprometidos y obtener credenciales almacenadas de forma insegura. Siguiendo a Caballero y Cilleros, algunos puntos críticos que podrían ser explotados son las credenciales en ficheros, las credenciales en el registro, la *bash history*, las claves privadas, la instancia de *cloud* de metadatos API y las preferencias de políticas de grupo.

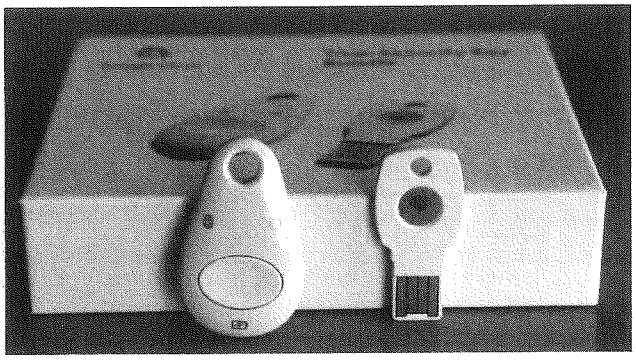


Imagen 13[531]. El *Google Titan Security Key* es un *token* de seguridad que permite añadir una capa de protección a los dispositivos.

531 La imagen fue descargada de CNBC. *Google's new $50 gadget is the best way to keep your accounts safe*, publicado el 30 de agosto de 2018. https://www.cnbc.com/2018/08/29/google-titan-security-key-review.html

5.8. LAS SITUACIONES DE JUSTIFICACIÓN EN EL DELITO DE ACCESO ILÍCITO

Finalmente, la antijuricidad se ve reforzada con el elemento *ilegítimamente*, ya que se sancionan únicamente las conductas que no tienen una causa de justificación. Al igual que con la voz *deliberada*, considero que su inclusión es innecesaria, pues en Perú estos supuestos se encuentran recogidos en el artículo 20 CP. Los párrafos 47 y 48 del Informe Explicativo del Convenio precisan por qué se sugirió su inclusión en el derecho interno:

> El acto debe también ser cometido de manera "ilegítima". Además de la explicación dada más arriba, este término implica que el acceso autorizado por el propietario o por otro tenedor legítimo del sistema o de parte del mismo no constituye delito (como, por ej., a los fines de efectuar una verificación autorizada o de proteger el sistema informático en cuestión). Por otra parte, no constituye delito el acceder a un sistema informático que permite el acceso libre y abierto del público, ya que tal acceso es "legítimo".
>
> La aplicación de instrumentos técnicos específicos puede dar lugar a un acceso conforme al Artículo 2, tal como el acceso a una página web, de manera directa o a través de enlaces de hipertexto, incluidos enlaces ocultos o la aplicación de "cookies" o "robots" para ubicar y recuperar información en aras de la comunicación. La aplicación de tales instrumentos no es *per se* "ilegítima". El mantenimiento de un sitio web público implica el consentimiento por parte del propietario del sitio web que cualquier otro usuario de red podrá acceder al mismo. La aplicación de las herramientas estándar provistas en los protocolos y programas de comunicación que comúnmente se aplican no es en sí misma "ilegítima", en particular cuando se puede considerar que el tenedor legítimo del sistema al que se acceder ha aceptado su publicación, por ej., en el caso de las "*cookies*" al no rechazar la instalación inicial o por no eliminarla.

De otro lado, es importante tomar en consideración que el artículo 12 LDI establece como causas de justificación actividades propias de la seguridad informática: "Está exento de responsabilidad penal el que realiza las conductas descritas en los artículos 2, 3, 4 y 10 con el propósito de llevar a cabo pruebas

autorizadas u otros procedimientos autorizados destinados a proteger sistemas informáticos".

Algunos autores consideran que el artículo 12 LDI recoge la figura del *hacker* ético[532], *hacker* de sombrero blanco o *white hat*[533]. En estos casos, expertos en seguridad informática analizan o testean las falencias de las redes a través de sus sistemas de bloqueo, *firewalls*, entre otros. Como bien señala Palazzi, la seguridad informática no es una disciplina acabada, por lo que "la única forma de detectar vulnerabilidades en los sistemas informáticos es buscándolas, testeando las fallas y reparándolas. Por eso es muy importante compartir información y experiencias en la materia y a ella apuntan, entre otras razones, las propuestas de blanquear en todo momento las fallas de seguridad de un sistema operativo"[534].

5.8.1. *Penetration test y vulnerability assessment*

Como se ha indicado anteriormente, en seguridad informática se busca fortalecer la confidencialidad, disponibilidad e integridad de los sistemas informáticos. Para ello, existen diversos procedimientos que analizan las falencias, vulnerabilidades y errores de configuración, con la finalidad de reportarlas a su titular[535]. A continuación, conoceremos uno de ellos.

Es importante que el lector diferencie el *penetration test* del *vulnerability assessment*. En este sentido, será importante conocer sus fases o etapas:

532 Espinoza Calderón, *Delitos informáticos y nuevas modalidades delictivas*, cit., p. 75.

533 Meneses Gonzáles/Meneses Ochoa, *La cibercriminalidad: Consideración criminológica, político-criminal, dogmática, procesal y cooperación internacional*, cit., p. 309.

534 Palazzi, "El delito de acceso ilegítimo a un sistema informático", cit., p. 47.

535 En el desarrollo de este acápite sigo, principalmente, el trabajo de Reale, "Importancia de la instrumentalización jurídica de la *vulnerability assesment* y la etapa de explotación de vulnerabilidades para evitar su criminalización", cit., pp. 54-80.

Paso 1. Búsqueda de información

- *Information gathering* o fase de reconocimiento: Se recolecta todo tipo de información, empleando fuente abierta, inspecciones físicas, entrevistas personales. Esto permite detallar y precisar el objetivo.

Paso 2. *Vulnerability assessment* o búsqueda de vulnerabilidades

- Se buscan las deficiencias, ausencias, debilidades de seguridad y vectores de ataque en el objetivo. Esta fase es importante, pues muchas veces se emite un informe exclusivo.
- Para su ejecución, pueden emplearse escáneres automatizados, pasivos y activos que realizan el procedimiento.

Paso 3. Explotación

- El actor intenta aprovechar las vulnerabilidades detectadas con la finalidad de acceder al sistema o realizar algún tipo de ataque que demuestre la importancia de corregir la deficiencia advertida.
- Así como hay diferentes tipos de vulnerabilidades, no todas son explotables. De este modo, dependerá de cada caso concreto.
- La explotación se realiza con códigos informáticos denominados *exploits*. Algunos permitirán explotar la vulnerabilidad, mientras que otros, interactuar con esta.

Paso 4. Elevación

- Se busca escalar permisos desde el sector del objetivo accedo y buscar privilegios o credenciales de administrador.

Paso 5. Post explotación

- Engloba acciones de pivoteo, entender el entorno, su funcionamiento, ver objetivos similares, analizar los perímetros de seguridad, entre otros.

Paso 6. Persistencia

- El objetivo es acceder al sistema informático, sin necesidad de repetir todas las acciones efectuadas previamente. Para ello, se genera un canal, acceso o puerta trasera que permite el acceso de forma indetectable.
- Si la vulnerabilidad es corregida con un parche, esta puerta trasera demostrará que los problemas subsisten.

Paso 7. Limpieza

- Se eliminan los rastros del acceso, así como toda huella que se haya dejado.
- Se elabora un informe que grafique lo descubierto, lo realizado, la manera de corrección, la tecnología empleada y otros contenidos.

Esquema 1. Etapas de un *penetration test*. Elaborado a partir de REALE, Julián. Op. Cit. pp. 55-59.

Como se puede apreciar, cada tópico de la autorización -sea a través de un contrato o de un *bug bounty*- es sumamente importante, razón por la cual se recomienda establecer los términos contractuales de forma clara y expresa: partes, objeto, forma procedimental de realizar el objeto y procedimiento, derechos y deberes de cada una de las partes, responsabilidad del proveedor,

detalles técnicos y targets, autorizaciones y no ejercicio de acciones penales, recursos, alcances y características del informe final, anexos[536].

Luis Angulo Aguirre, ingeniero industrial de la Pontificia Universidad Católica del Perú (PUCP) y catedrático en la Universidad Nacional de Ingeniería (UNI) y la Universidad Tecnológica del Perú (UTP), publicó *Hacking & Cracking*, un libro que, aunque contiene abundante información técnica, la presenta de manera sencilla y con ejemplos claros que facilitan la comprensión de conceptos altamente especializados. A continuación, transcribo un ejemplo de informe técnico diseñado por el autor, en el que emplea una brillante analogía:

16 de febrero de 2019	Informe técnico
Para	Lic. Olga Emily Cazún Directora Deptal de Educación Francisco Javier Magaña Coordinador de seguimiento a la calidad
De	Lic. José Adalberto Martínez Alfaro Asesor Pedagógico Distrito 03-17
Lugar y fecha	CE Cas. Belén C/Suncita
Descripción de la situación	Denuncia hecha por teléfono a Asesor de Gestión Francisco Martínez que los maestros/as del CE Cas. Belén C/Suncita no estaban trabajando con alumnos por realizar una actividad dentro de la escuela.
Observaciones	Al momento de la visita, todos los docentes estaban trabajando con alumnos/as en sus aulas. Estaban personas de PRONIÑO entregando mochilas y cuadernos a algunos padres y madres de familia, pero estos no interrumpían las clases, ya que lo hacían en la dirección de la escuela. Estaban padres de alumnos de CDE haciendo ventas en la cocina y vendían en los recreos, habían pedido a la señora de la tienda que les dejara vender ese día, según informan no tienen ni para fotocopias. Según la Directora del centro escolar Edelmira Bolaños, esa denuncia llamó la atención por no cuidar su zona en horas de recreo. Esa misma versión la sostiene una madre de familia del CDE. Estaban personas de PRONIÑO entregando mochilas y cuadernos fuera del CDE, alumnos y miembros del CDE que se encontraban en la escuela en dicha actividad, quienes lamentaron que se den situaciones de este tipo.
Anexos	Copia de acta firmada por miembros CDE Ficha de Registro de Asistencia

Cuadro 18. Informe técnico. Elaborado por Luis Angulo Aguirre[537].

El paralelismo que el autor utiliza puede ser interpretado de la siguiente forma:

536 Los aspectos detallados han sido desarrollados por Reale, "Importancia de la instrumentalización jurídica de la *vulnerability assesment* y la etapa de explotación de vulnerabilidades para evitar su criminalización", cit., pp. 70-78.

537 Angulo Aguirre, *Hacking & cracking – Redes inalámbricas Wi-Fi*, cit., p. 28.

- Los docentes que trabajan en sus aulas representan los programas o aplicaciones que funcionan de forma correcta, sin ningún tipo de interferencia o riesgo.
- Proniño entregando mochilas y cuadernos simboliza la transferencia de datos o información en un ambiente autorizado y controlado.
- Los padres que realizan ventas autorizadas por la institución simulan ser programas de terceros, pero que funcionan de forma limitada con la autorización del titular.
- La directora preocupada por la falta de control durante el recreo grafica la necesidad de incrementar la supervisión durante las horas de mayor tráfico de datos.
- Finalmente, la entrega de material fuera del colegio por parte de una entidad autorizada (Proniño) ejemplifica a los *insiders* o empleados que comparten datos de la empresa sin cifrar o de forma poco segura.

5.8.2. ¿Acceso ilícito en ejercicio de la patria potestad?

Actualmente, el *grooming* (proposición a niños, niñas y adolescentes con fines sexuales por medios digitales), la distribución de imágenes de explotación sexual de menores de edad (mal llamada *pornografía infantil*) y el *cyberbullying* (acoso a menores de edad) son actividades delictivas que generan alarma y preocupación en los padres de familia. En este contexto, ¿el papá o la mamá que ingresa a la cuenta de Facebook, Instagram o TikTok de su hijo, sin su autorización y con la finalidad de monitorear sus actividades en línea, comete acceso ilícito?



Imagen 14. MSpy es una aplicación de control parental cuyas funciones son invasivas[538].

538 Entre las funciones que el desarrollador destaca, pero que generan preocupación, tenemos: Ver chats privados en redes sociales, acceder de forma remota a la cámara

Como se ha dicho en esta obra, el delito de intrusismo informático protege la seguridad informática, específicamente, la confidencialidad de los usuarios; sin embargo, el derecho penal no debería ser un instrumento para destruir o deteriorar el núcleo familiar. Por esta razón, sería importante incluir una cláusula que incorpore ciertas excusas absolutorias para no criminalizar escenarios como el que acabo de describir. Al abordar la *intimidad informática*, el profesor Silva Sánchez describe este problema y defiende la solución -a la cual me adhiero-:

> El ejercicio responsable de la patria potestad, en el contexto social actual, adquiere una especial importancia en lo relativo al control de las comunicaciones de los hijos. En efecto, este control resulta imprescindible para su protección frente a las agresiones y adicciones de todo género a las que precisamente les expone la tolerancia estatal. Pues bien, ello requiere examinar periódicamente su teléfono móvil, su correo electrónico o sus accesos a internet. Por lo tanto, dada su adecuación al proyecto educativo familiar, una intervención así no puede calificarse como lesión típica de su intimidad. Ahora bien, aunque lo fuera, estaría justificada por la defensa de la integridad física y moral del menor. Ciertamente, se propuso una solución dogmática para los casos en los que la conducta de los padres constituye un injusto culpable. En concreto, la creación de una excusa absolutoria, que excluye la punibilidad de la conducta. De este modo, se pretende evitar la judicialización de las relaciones familiares. Ciertamente, la injerencia de cualquier orden jurisdiccional en la vida familiar es mala en general para esta. Sin embargo, en concreto la intervención del Derecho penal es catastrófica, dado que puede producir la ruptura definitiva de la comunidad paternofilial -en virtud del ingreso en prisión o de las prohibiciones de comunicación de larga duración-. Así pues, la propuesta de una excusa absolutoria es ciertamente razonable para los casos en que se aprecie un injusto típico y culpable que no alcance a constituir una grave forma de violencia doméstica. Con todo, su introducción no

---

del dispositivo, activar el micrófono para realizar grabaciones a distancia, leer textos y mensajes de correos electrónicos, acceder a fotos y videos, a distancia, rastrear la ubicación, leer lo que escriben a través de *keylogger*, alertar de palabras clave, realizar capturas de pantalla, entre otros.
La imagen y el contenido ha sido obtenido de: https://www.mspy.com/es/

obsta a lo señalado antes en el sentido de que exista un claro espacio de conformidad a Derecho en las conductas educativas de los padres[539].

5.9. CONSUMACIÓN

A nivel nacional, la doctrina sostiene casi de manera unánime que el acceso ilícito constituye un delito de mera actividad[540] y, por tanto, no admite tentativa[541]. En esta línea, el profesor Oré Sosa señala que el intrusismo informático debe considerarse un delito de consumación anticipada[542]. No obstante, García León plantea una perspectiva distinta, al afirmar que la vulneración de las medidas de seguridad transforma el acceso ilícito en un delito de lesión, el cual sí admite la tentativa:

> [...] si el acceso se daría con tan solo un *click* o solo presionando la tecla *enter*, que en segundos o microsegundos permite el acceso al sistema informático se haría más difícil apuntar a una hipótesis de tentativa.
>
> Sin embargo, conociendo el incremento de la propagación de este tipo de delitos, y por ende la preocupación de empresas privadas, nacionales y transnacionales de perfeccionar sus barreras de seguridad, la labor del agente requerirá cierto tiempo o ir superando barrera por barrera de seguridad para ingresar al sistema y este intento puede calificar como el inicio de la ejecución punible de este delito[543].

539 Silva Sánchez, Jesús-María. *Derecho penal. Parte general.* Madrid: Civitas, 2025, p. 1578.

540 "Según la consumación del delito: Este delito sería uno de mera actividad en la medida que el hecho de acceder ilegítimamente a un sistema informático o a parte de él, implicaría la consumación del delito. Basta que el sujeto haya accedido a un sistema informático o a parte del mismo" (Arévalo Minchola/Vega Aguilar, *Ciberdelitos. Análisis en el sistema penal*, cit., p. 261). En la misma línea: Jiménez Herrera, *Manual de derecho penal informático*, cit., p. 408; Espinoza Calderón, *Delitos informáticos y nuevas modalidades delictivas*, cit., p. 74; Rodríguez Rocha, "El delito de acceso ilícito a los sistemas informáticos. Análisis del tipo penal y el rol de la cooperación judicial internacional", cit., p. 344.

541 Meneses Gonzáles/Meneses Ochoa, *La cibercriminalidad: Consideración criminológica, político-criminal, dogmática, procesal y cooperación internacional*, cit., p. 308.

542 Oré Sosa, *Delictum. Apuntes de derecho penal*, cit., p. 193.

543 García León, "Análisis del tipo de acceso ilícito. Bien jurídico, tipicidad objetiva y subjetiva, autoría y participación, y su distinción con el delito de atentado a la integridad de datos y sistemas informáticos", cit., p. 372.

A nivel comparado, en Argentina, por ejemplo, se discute si la tentativa es reprochable o no[544]. Para ello, se plantean algunos ejemplos[545]:

- **[Caso 63]** Un delincuente se encuentra en la fase de descubrimiento y detección de vulnerabilidades, pero en ese momento el IDS o Sistema de Detección de Intrusos de la empresa advierte su presencia, alerta al departamento de Tecnología de la Información y cierran las conexiones o puertas de ingreso.

- **[Caso 64]** Un delincuente utiliza un programa de ataque de *fuerza bruta*, es decir, introduce, en muy poco tiempo y de forma sucesiva, cientos o miles de posibles contraseñas. Mientras el programa está corriendo e intentando descifrar la clave correcta, ¿ya comenzó la ejecución y, en consecuencia, el *iter criminis* podría ser interrumpido?

Desde mi perspectiva, lo primero que debe analizarse es el bien jurídico que se busca proteger. En aquellas legislaciones que incluyen este delito dentro del capítulo *De delitos contra el patrimonio*, se le considerará un delito de peligro, ya que el mero acceso indebido no genera un daño directo al patrimonio. Algo similar ocurre con la integridad informática, pues el acceso ilícito, por sí solo, no la afecta, aunque en ciertos casos podría comprometerla.

544 "También se lo presenta como un tipo de mera actividad y de peligro, advirtiendo incluso que incorrectamente interpretado podría constituirse en una suerte de acto preparatorio punible con olvido del principio de lesividad. La tentativa es posible: basta con pensar en los casos de uso de programas que operan por fuerza bruta, es decir, introduciendo sucesivamente todas las posibles alternativas de combinación alfanuméricas que constituyen una clave, supuestos en los que podría interrumpirse el "iter" entre el comienzo de la ejecución y la consumación" (Riquert, Marcelo A. "El acceso ilegítimo a sistema o dato informático [art. 153 bis del Código Penal]". En: Dupuy, Daniela [dir.] y Mariana Kiefer [coord.]. *Cibercrimen. Aspectos de derecho penal y procesal penal. Cooperación internacional. Recolección de evidencia digital. Responsabilidad de los proveedores de servicios de Internet.* Montevideo: B de F, 2019, p. 242).

545 Los ejemplos han sido tomados de Reale, "Importancia de la instrumentalización jurídica de la *vulnerability assesment* y la etapa de explotación de vulnerabilidades para evitar su criminalización", cit., pp. 66 y s.

No obstante, en este texto se plantea que el bien jurídico protegido es la seguridad informática. Desde esta óptica, la confidencialidad de los datos y sistemas informáticos es un componente esencial de dicha seguridad. En consecuencia, cualquier acción que vulnere la confidencialidad supondrá una lesión directa al bien jurídico que se pretende resguardar.

Dicho esto, según su redacción y ubicación en la legislación peruana, el acceso ilícito es un delito de resultado y, en consecuencia, la tentativa es posible. Esta interpretación permite castigar los casos 62 y 63, así como a aquellas situaciones en las que se introduce un factor de autenticación, pero el sistema bloquea el acceso por la falta del segundo.

5.10. CONCURSOS

Son muy pocos los autores que han abordado situaciones concursales en el ámbito de la delincuencia informática dada su alta complejidad. De este modo, será una labor que, desde la doctrina y la jurisprudencia, debemos empezar a desarrollar:

> Finalmente, es necesario analizar el complejo tema del concurso de tipicidades (aparente o efectivo) en los delitos informáticos. El tema es difícil porque el legislador colombiano ha diseñado un esquema progresivo de las figuras cibercriminales, pues entre ellas existe una relación de medio a fin o de actos preparatorios a consumados dentro del *iter criminis*, lo que genera complejos solapamientos hermenéuticos a la hora de interpretar el verdadero alcance de los injustos realizados por el autor. Se trata de situaciones que demuestran un abuso legislativo del adelantamiento de las barreras de protección de la seguridad de la información, los datos y los sistemas informáticos[546].

A nivel local, en algunos casos de acceso ilícito, Lizet Rodríguez advierte concurso real con la comisión del delito de fraude informático[547].

---

546 Posada Maya, Ricardo. *Los cibercrímenes: Un nuevo paradigma de criminalidad. Un estudio del título VII bis del Código Penal colombiano*. Bogotá: Grupo Editorial Ibáñez, 2017, p. 267.

547 Rodríguez Rocha, "El delito de acceso ilícito a los sistemas informáticos. Análisis del tipo penal y el rol de la cooperación judicial internacional", cit., p. 344.

De otro lado, para Godofredo García existirá concurso aparente entre el delito de acceso ilícito y los delitos de atentados contra la integridad de datos y sistemas informáticos, ya que, en su opinión, "el delito de acceso ilícito funcionaría como una especie de acto preparatorio"[548]. Sin embargo, este autor considera que, si los dos ataques están distanciados temporalmente, se podría hablar de un concurso real de delitos[549].

En los delitos informáticos, en muchas ocasiones tendremos problemas para construir la imputación y, en consecuencia, determinar situaciones concursales. Por ejemplo:

[Caso 65] Jorge ingresa a Google, digita las palabras *Banco de confianza* y le da clic al primer resultado. Sin darse cuenta, accede a una página suplantadora, ingresa sus datos (usuario y contraseña), trata de realizar alguna transacción, pero no puede. Algunas horas después, al revisar su estado de cuenta, ve que le han sustraído diez mil soles. Inmediatamente llama a su banco y le indican que el dinero fue transferido a Ámbar.

En el caso podemos advertir varias conductas ilícitas:

a. Suplantación de identidad (art. 9 LDI) al simular una página web.
b. Atentado contra la integridad de sistemas informáticos (art. 4 LDI) al desviar el tráfico de un sistema a otro.
c. Interceptación de datos informáticos (art. 7 LDI) al interceptar u obtener el usuario y contraseña que digita.
d. Acceso ilícito (art. 2 LDI) al emplear los datos de Jorge para ingresar a la cuenta veraz.
e. Fraude informático (art. 8 LDI) al realizar las transferencias a favor de Ámbar.

Los delitos informáticos representan un gran desafío para la dogmática penal y para el razonamiento probatorio. Así, muchas veces, se le imputa el

548 García León, "Análisis del tipo de acceso ilícito. Bien jurídico, tipicidad objetiva y subjetiva, autoría y participación, y su distinción con el delito de atentado a la integridad de datos y sistemas informáticos", cit., p. 374.

549 *Ibid.*, p. 375.

delito de fraude informático y otros tantos a la cuenta receptora (*cibermula*). El problema es que, en la investigación, se asume que la cuenta beneficiaria sería la responsable de todos los actos que hemos descrito previamente, cuando, en realidad, solo sabemos que recibió la transferencia.

Espero, en una próxima publicación, proponer una metodología adecuada para la investigación criminal, que inicie con el diseño de hipótesis razonables y que concluya con una adecuada valoración de la prueba -sea digital o no-. Ahora bien, en el caso bajo análisis, ¿qué podría haber sucedido? Ensayaré tres de las muchas hipótesis posibles:

Hipótesis 1. Ámbar diseñó una página web suplantadora, la posicionó de tal forma que sea el primer resultado que aparece al *googlearla*, almacenó los datos enviados por la víctima -sin que esta lo sepa- al ingresar a la web falsa, los empleó para acceder a la cuenta bancaria de la víctima y realizarse la transferencia.

Hipótesis 2. El ciberdelincuente A diseñó la página web falsa y la posicionó en Google para que sea la primera opción que apareciera. Registró la información de cientos o miles de usuarios que ingresaron a la página maliciosa. Vendió dicha información. El ciberdelincuente B compró un *paquete* en el que se encontraba la información de Jorge. Con la información, ingresa a la cuenta y realiza la transferencia a favor de Ámbar.

Hipótesis 3. El ciberdelincuente A se dedica al diseño de páginas web falsas de bancos peruanos. El ciberdelincuente B adquiere los archivos fuente de la página suplantadora en un archivo zip. El ciberdelincuente C obtiene el dominio y el *hosting* que alojará la página suplantadora. Cuando la página suplantadora ya está en línea, el ciberdelincuente D compra las credenciales que le permiten administrar la página web y, de este modo, apoderarse de una enorme base de datos (usuarios y contraseñas). El ciberdelincuente E adquiere el registro de 100 usuarios -entre los cuales se encuentra nuestra víctima-, los utiliza, accede a su sistema y realiza la transferencia a favor de Ámbar.

Como se puede apreciar, estas hipótesis generan problemas tanto de autoría y participación como concursales[550]. Por esta razón, la fiscalía debe re-

550 "Mientras la teoría de la participación trata el caso en el que varias personas realizan un tipo, la teoría del concurso se ocupa de los casos inversos, en los que una persona

cabar elementos de prueba y, con estos, construir una hipótesis que le permita imputar el hecho a una o más personas.

A continuación, planteo tres circunstancias que configuran supuestos de *concurso ideal*, pues si bien temporalmente se producen uno después de otro, en realidad estamos frente a una unidad de hecho típico, esto es, una decisión volitiva unitaria de actos realizados dentro de un mismo acontecimiento[551]:

- Si el delincuente instala un *keylogger* para acceder a las pulsaciones del teclado y luego accede al sistema informático de la víctima con el usuario y contraseña que obtuvo de esta forma.
- Si el delincuente accede al sistema informático, vulnerando las medidas de seguridad, y luego elimina algunos datos informáticos que identificó como objetivo.
- Si el delincuente accede al sistema informático, cambia sus privilegios de usuario, se coloca como administrador y toma el control del sistema, impidiendo que los legítimos usuarios accedan.

5.11. PENALIDAD[552]

Desde el 2023, cuando el acceso ilícito se comete sin vulnerar medidas de seguridad, sea accediendo o excediendo lo autorizado, el autor será castigado

realiza varios tipos" (Roxin, Claus. *Derecho penal parte general.* T. II: *Especiales formas de aparición del delito.* Navarra: Thomson Reuters / Aranzadi, 2014, p. 942).

551 "Se trata de conductas sucesivas cuando el autor realiza *varios actos sucesivos* (uno detrás de otro) que están orientados a la consecución de un fin delictivo ulterior. Dentro de este ámbito se encuentran tanto la pluralidad de actos sucesivos que están vinculados con un injusto penal consumado como la pluralidad de actos que están relacionados con una tentativa sucesiva" (Salazar Sánchez, Nelson. "Concurso ideal de delitos". En: Salazar Sánchez, Nelson [dir.]. *Comentarios al Código Penal peruano. Parte general*, t. III. Lima: Gaceta Jurídica, 2019, p. 47).

552 En el 2014, se afirmaba que el acceso ilícito es "un comportamiento sobre el que se discute si realmente es necesaria la intervención del derecho penal o bastaría con la del contravencional o sancionador administrativo, apareciendo como más lógicas las penas pecuniarias o de inhabilitación que la prisión" (Riquert, Marcelo [coord.]. *Ciberdelitos: Grooming, stalking, bullying, sexting, ciberodio, propiedad intelectual, problemas de perseguibilidad, ciberpornografía infantil.* Buenos Aires: Hammurabi, 2014, p. 52).

con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa. Estamos frente a dos clases de pena que deben ser impuestas conjuntamente.

En cambio, cuando el acceso ilícito se realiza vulnerando las medidas de seguridad, la sanción oscila entre tres y seis años y ochenta y ciento veinte días-multa.

Sobre este punto, en una eventual reforma legislativa sería importante analizar el *quantum punitivo* del castigo, ya que parecería ser desproporcional respeto a otro tipo de conductas cuyo desvalor es menor[553].

5.12. CIRCUNSTANCIAS AGRAVANTES

Son aplicables las cinco circunstancias previstas en el artículo 11 LDI:

i) Cuando el acceso ilícito se comete como integrante de una organización criminal.

Actualmente, diferentes organizaciones criminales reclutan a quienes tienen habilidades y destrezas para acceder a sistemas informáticos y obtener información que será empleada para cometer otros ciberdelitos como *ransomware*, sabotaje informático, fraude informático, entre muchos otros.

553 En la misma línea: "En tercer lugar, es cuestionable que el quantum punitivo sea ínfimo con relación a las penas que se imponen a otros delitos cuya lesividad al bien jurídico puede ser menos significativa. Siguiendo la descripción actual de los tipos penales en cuestión, un ciberatacante podría ser condenado a una pena de prisión menor a cuatro años, lo cual de acuerdo al sistema penal peruano de penas podría significar la suspensión de la ejecución de la pena efectiva y su reemplazo por reglas de conducta [...] Es decir, el tratamiento legislativo cuantitativo de las sanciones punitivas debe guardar estrecha relación con el mayor o menor desvalor del comportamiento tipificado. Cuando no se cumple con esto último no se consigue transmitir un mensaje serio de persecución contra la ciberdelincuencia" (Requejo Passoni, Wendy. "Avances y retrocesos de la política criminal relativa a los delitos contra datos y sistemas informáticos en el Perú". En: Caro Coria, Carlos Dino y Luis Reyna Alfaro [dir.]. *Ciberseguridad, cibercrimen y nuevas tecnologías. Riesgos y respuestas jurídicas*. Ciudad de México: Derecho Global Editores, 2022, pp. 52 y s).

[Caso 66] En los últimos años, se ha descubierto que organizaciones dedicadas al narcotráfico comenzaron a reclutar ciberdelincuentes para infiltrarse en sistemas informáticos y así localizar rápidamente los cargamentos de droga enviados a Europa. Un caso emblemático ocurrió en 2011, cuando se comprobó que una red criminal vulneró los sistemas del puerto de Amberes, en Bélgica, para identificar narcóticos ocultos en contenedores que, en apariencia, transportaban plátanos procedentes de Sudamérica[554].

ii) Cometer el delito mediante el abuso de una posición especial de acceso a la data o información reservada o al conocimiento de esta información en razón del ejercicio de un cargo o función.

Los *insiders* son miembros de una organización, empresa o institución que aprovechan su posición, al interior, para facilitar, proporcionar o brindar información a usuarios que no deberían acceder a esta[555].

[Caso 67] Según un informe de la compañía de ciberseguridad Kaspersky, ciberdelincuentes reclutan *insiders* o personas con información privilegiada para obtener acceso a las redes de telecomunicaciones y a los datos de los abonados. Según la investigación, en el 28 % de los ataques cibernéticos y el 38 % de los ataques dirigidos intervienen funcionarios o trabajadores que cuentan con información privilegiada[556].

554 Infobae. *Narcos y hackers, cómo funciona esta nueva alianza delictiva que crece en la oscuridad*, publicado el 4 de noviembre de 2018. https://www.infobae.com/america/mexico/2018/11/02/narcos-y-hackers-como-funciona-esta-nueva-alianza-delictiva-que-crece-en-la-oscuridad/

555 En esta línea, la literatura lo define como "cibercriminal que pertenece o trabaja para la institución o empresa víctima de la infracción" (Miró Llinares, *El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio*, cit., p. 305).

556 "Cibercriminales reclutan a personas con información privilegiada para atacar a los proveedores de telecomunicaciones, en *Kaspersky*, 20 de setiembre de 2016. https://

De este modo, si el miembro de una empresa o una institución pública es contratado por terceros para que brinde acceso a los sistemas informáticos y este -en atención a su posición e información privilegiada- lo hace, incurrirá en esta circunstancia agravante[557].

iii) Cometer el delito con la finalidad de obtener un beneficio económico. Por ejemplo, si se logra el acceso a sistemas que albergan información relacionada secretos industriales o la actuación de la empresa competidora, nos encontraremos frente a "espionajes industriales", a través de los cuales se busca lograr una mejor posición o ganancia económica[558].

iv) Comprometer fines asistenciales, la defensa, la seguridad y la soberanía nacionales.

[Caso 68] Turla es un grupo de ciberespionaje activo desde el 2010, aproximadamente, que ha puesto en riesgo la confidencialidad de entidades diplomáticas de diversos países. Opera a través de la difusión de *malware* que permite acceder a información confidencial y, luego, exportarla a Dropbox.

En el 2020, investigadores de ESET descubrieron un conjunto de herramientas de *malware* que permiten implementar puertas traseras (*backdoors*) y, de este modo, acceder y recolectar documentos confidenciales. Se sabe que este grupo de ciberdelincuentes han comprometido miles de sistemas pertenecientes a gobiernos, embajadas e instalaciones educativas y de investigación de más de 100 países. Siendo esto así, sus ataques vulneran medidas de seguridad

latam.kaspersky.com/about/press-releases/cibercriminales-reclutan-a-personas-con-informacion-privilegiada-para-atacar-a-los-proveedores-de-telecomunicaciones

557 Para García León ("Análisis del tipo de acceso ilícito. Bien jurídico, tipicidad objetiva y subjetiva, autoría y participación, y su distinción con el delito de atentado a la integridad de datos y sistemas informáticos", cit., p. 373), este supuesto configura un caso de complicidad primaria, "pues su aporte será esencial y en etapa de preparación".

558 Davara Fernández de Marcos/Davara Fernández de Marcos, *Delitos informáticos*, cit., p. 34.

con la finalidad de acceder a información que podría estar vinculada con la defensa, la seguridad o la soberanía nacional[559].

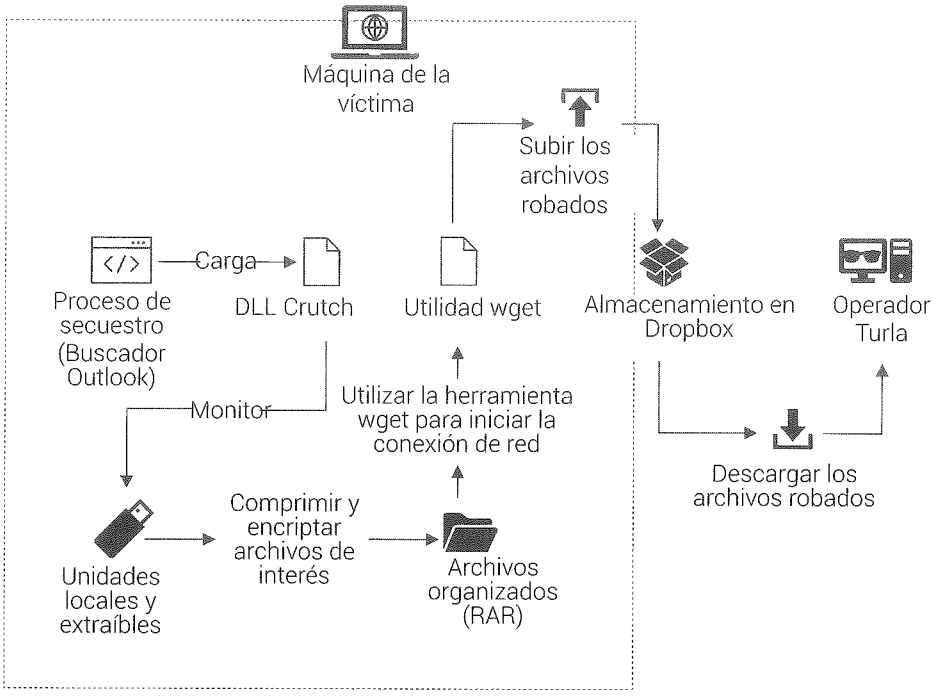


Diagrama 9. Ataque de exfiltración de datos. Adaptación.

En Argentina, algunos autores destacan la importancia de esta circunstancia agravante y cuestionan que su legislación local no sancione con mayor severidad ataques que se dirigen contra infraestructuras críticas -aquellas que sustentan servicios esenciales como energía, transporte, salud, seguridad y defensa-[560]. Una eventual

559 Centro Nacional de Seguridad Digital. *Alerta integrada de seguridad digital N.º 242-2020.* Lima: 2 de diciembre de 2020, p. 8. https://www.gob.pe/institucion/pcm/informes-publicaciones/1369751-alerta-integrada-de-seguridad-digital-n-242-2020-pecert. Además, ESET. *Crutch: nuevo backdoor de Turla utilizado para exfiltrar documentos vía Dropbox*, publicado el 2 de diciembre de 2020. https://www.welivesecurity.com/la-es/2020/12/02/crutch-nuevo-backdoor-turla-exfiltrar-documentos-dropbox/

560 "En futuras reformas se debería modificar esta agravante, a fin de incluir infraestructuras críticas que, con la redacción vigente del tipo penal, han quedado excluidas como las infraestructuras de salud, seguridad, servicios esenciales, correos,

reforma de nuestro ordenamiento exige debatir la fórmula empleada por el legislador peruano.

v) Cometer el delito empleando la inteligencia artificial o tecnologías similares o análogas (conforme a la Ley N.º 32314).

5.13. PROPUESTA NORMATIVA

A partir del análisis expuesto en este capítulo, propongo modificar el delito de acceso ilícito, tomando en consideración:

i. Eliminar los elementos *deliberada* e *ilegítimamente*.

ii. Excluir los accesos ilegales sin vulneración de medidas de seguridad.

iii. Incluir un elemento subjetivo trascendente como recoge el ordenamiento chileno.

iv. Precisar el alcance del acceso ilícito, generado por el abuso de confianza, siguiendo la fórmula de Argentina, Colombia, España, y República Dominicana.

v. Modificar el rango de la sanción penal.

De este modo, el delito de acceso ilícito propuesto se regularía en los siguientes términos:

> **Art. 2.- Acceso ilícito**
>
> El que accede a todo o parte de un sistema informático, con la finalidad de obtener datos informáticos u otra intención delictiva, mediante la vulneración de las medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con treinta a noventa días-multa.
>
> Será reprimido con la misma pena, el que, con la finalidad de obtener datos informáticos u otra intención delictiva:

---

energía, etc., ya que la enumeración del art. 153 bis es imprecisa, y no detallada como la ley española" (Garat, Sebastián y Julián Reale. "La reforma penal en materia de cibercrimen en la República de Argentina". En: Dupuy, Daniela [dir.]. *Cibercrimen II. Nuevas conductas penales y contravencionales. Inteligencia artificial aplicada al derecho penal y procesal penal. Novedosos medios probatorios para recolectar evidencia digital. Cooperación internacional y victimología*. Montevideo: B de F, 2018, p. 513).

1. Accede a todo o parte de un sistema informático excediendo lo autorizado.
2. Se mantiene en un sistema informático contra la voluntad de quien tenga el legítimo derecho a excluirlo.

5.14. CONCLUSIONES DEL CAPÍTULO

- El acceso ilícito es una de las principales amenazas a la seguridad informática. Todos los ciudadanos, las organizaciones y las empresas son vulnerables a los ciberataques: no existe la seguridad absoluta. Por esta razón, la resiliencia ante ataques informáticos es clave para la continuidad de las operaciones comerciales y la protección de la información.
- La investigación del intrusismo informático es compleja debido a la volatilidad de la prueba digital y la necesidad de conocimientos técnicos avanzados. Si bien existen fiscalías especializadas en ciberdelincuencia en Lima Centro, La Libertad y Arequipa, en el resto del país las investigaciones dependen de fiscalías penales comunes que requieren capacitación especializada y mejores recursos logísticos.
- Existen problemas estructurales para mejorar la investigación del intrusismo informático. Por ejemplo, la falta de claridad en la redacción de las actas (en ocasiones, no se precisa el número de víctimas ni el objetivo del ciberdelincuente), ausencia de detalles técnicos (no se especifica cómo ocurrió el acceso ilícito ni qué medidas de seguridad fueron vulneradas), no se indaga sobre las medidas de protección (no se pregunta si la víctima usaba autenticación en dos pasos, si compartía contraseñas, etc.).
- El impacto de casos mediáticos demuestra cómo la presión social puede generar avances legislativos en la protección de la seguridad informática. Un caso emblemático ocurrió en Brasil, pues el ataque informático contra la actriz Carolina Dieckmann originó la tipificación de los delitos informáticos en dicho ordenamiento (2012).
- El Convenio de Budapest define el acceso ilícito como el ingreso deliberado e ilegítimo a un sistema informático, permitiendo que los países decidan si exigen medidas de seguridad como requisito

para configurar el delito. De otro lado, la Convención de las Naciones Unidas contra la Ciberdelincuencia adopta una fórmula similar, pero hace referencia a *sistemas de tecnología de la información y las comunicaciones*, en lugar de *sistemas informáticos*.

- A partir del estudio y revisión de la legislación latinoamericana comparada, se puede afirmar que cada país ha tipificado el acceso ilícito de manera distinta, con diferencias en la ubicación en el Código Penal (algunos lo consideran delito contra la seguridad informática, mientras que otros, contra la privacidad o el patrimonio), los elementos del tipo penal (algunos países exigen vulneración de medidas de seguridad, mientras que otros sancionan cualquier acceso no autorizado) y los elementos subjetivos trascendentes (algunos castigan con penas mayores si el acceso se hace con intención de cometer otros delitos).
- Sobre la evolución de este delito en Perú, es importante precisar que, en el 2000, el Código Penal incluyó por primera vez el delito de acceso indebido en el artículo 207-A, pero exigía una finalidad económica. En 2013, la LDI incorporó un tipo penal más amplio, pero solo castigaba accesos que vulneraran medidas de seguridad. En 2014, se agregaron los términos *deliberada* e *ilegítimamente*, aunque su inclusión aún genera debates sobre su necesidad. En 2023, la última reforma eliminó el requisito de vulneración de medidas de seguridad para configurar el delito base, lo que amplió su alcance.
- Existe un férreo debate sobre el bien jurídico protegido en el delito de acceso ilícito. Así, algunos consideran que se tutela la privacidad o la confidencialidad de la información. Otros sostienen que su objetivo es garantizar la seguridad informática en general y la confidencialidad en particular.
- La seguridad informática es un bien supraindividual que protege tanto derechos individuales (intimidad, patrimonio, información) como colectivos (infraestructura crítica, información gubernamental).
- Actualmente, el artículo 2 LDI castiga dos escenarios: el acceso ilícito sin vulneración de medidas de seguridad o exceso de auto-

rización (la sanción oscila entre uno (1) y cuatro (4) años de pena privativa de libertad) y el acceso ilícito con vulneración de medidas de seguridad (la sanción va de tres (3) a seis (6) años de pena privativa de libertad).

CAPÍTULO 6

ATENTADO A LA INTEGRIDAD DE DATOS INFORMÁTICOS



* La ilustración de la página anterior corresponde a una adaptación de *Retrato de Joséphine Charlotte du Val d'Ognes*, de Marie-Denise Villers (1801). Para su elaboración, se empleó una de las herramientas de generación de imágenes de la empresa OpenAI.

CAPÍTULO 6

ATENTADO A LA INTEGRIDAD DE DATOS INFORMÁTICOS*

Sumario: 6.1. Introducción. 6.2. Regulación en el Convenio sobre la Ciberdelincuencia. 6.3. Regulación en la Convención de las Naciones Unidas contra la Ciberdelincuencia. 6.4. Legislación comparada. 6.5. Legislación nacional. 6.6. El bien jurídico penalmente protegido. 6.7. Tipicidad objetiva. 6.8. Tipicidad subjetiva. 6.9. Las situaciones de justificación en el delito de atentado contra los datos informáticos. 6.10. Consumación. 6.11. Concursos. 6.12. Penalidad. 6.13. Circunstancias agravantes. 6.14. Propuesta normativa. 6.15. Conclusiones del capítulo.

> Todas las empresas y organizaciones son vulnerables a los ciberataques. No existe la seguridad absoluta. Constantemente somos testigos de que los agentes más sofisticados están dispuestos a dedicar importantes fondos y recursos a los ciberataques. La capacidad de recuperarse con rapidez y continuar las operaciones comerciales podría marcar la diferencia entre el éxito y el fracaso de una organización.[561]

6.1. INTRODUCCIÓN

Apreciado lector, imagine que, luego de varios meses de trabajo, lágrimas de esfuerzo, entrevistas y reuniones periódicas con su asesor de tesis, alguien

---

* Algunas reflexiones y comentarios de este capítulo fueron publicadas en Elías Puelles, Ricardo. "Daños y sabotajes informáticos: ataques contra los datos y los sistemas informáticos". En: Caro Coria, Carlos; Luis Miguel Reyna Alfaro y Ricardo Elías Puelles (dirs.). *Ciberseguridad, cibercrimen, y AI LegalTech*. México: Derecho Global Editores, 2025.

561 Johnson, "Los profesionales de InfoSec deben aplicar la resiliencia operativa", cit., p. 24.

ingresa a su computadora, borra la carpeta que contiene todas las versiones de sus avances, luego, ingresa a su nube para eliminar, incluso, las copias de seguridad, y, finalmente, elimina de su disco duro y de sus USB todo rastro de la tesis. Debo reconocer que, en la redacción de este libro, ese fue uno de mis mayores temores: años de investigación que, por alguna extraña razón, pudiesen ser eliminados presencial o remotamente. Como sospechará, hice constantes copias y *backups*.

En este capítulo, estudiaremos el delito de atentado o ataque a la integridad de los datos informáticos. En la doctrina, este ilícito es conocido como *daños informáticos*, diferenciándose de los *daños a un sistema informático*, el cual corresponde al delito previsto en el artículo 5 del Convenio de Budapest. A nivel local, Perú recoge este delito con una ligera variación en su *nomen iuris*: *atentado contra la integridad de datos informáticos*. No obstante, antes de continuar, quisiera rememorar dos eventos históricos: uno ocurrido en la década de los ochenta y otro a fines del 2017.

[Caso 69] El 20 de setiembre de 1988, Texas amanecía con la primera condena por delito informático registrada en su sistema de justicia penal. Bajo el titular "Exprogramador culpable de plantar un virus", se relataba la historia de Donald Gene Burleson, quien utilizó un *malware* para eliminar 168 mil registros, luego de ser despedido de la firma de seguros y corretaje USPA e IRA Company. Así, el jurado del condado de Tarrant declaró culpable al encargado del área de seguridad informática, de 40 años, por la comisión de un delito grave de tercer grado, imponiéndole una pena de 10 años de prisión y una multa de cinco mil dólares[562].

[Caso 70] Petya apareció en el 2016 y era un *ransomware* que encriptaba archivos para, luego, requerirle a la víctima un pago en bitcoin para su liberación. Un año después, específicamente en junio del 2017, se diseminó

562 Aboso, *Derecho penal cibernético*, cit., p. 360; Deseret News. *Ex-programmer guilty of planting virus*, 20 de setiembre de 1988. https://www.deseret.com/1988/9/20/18778562/ex-programmer-guilty-of-planting-virus/

un *malware* similar bautizado como NotPetya, el cual afectó a más de dos mil compañías en Ucrania[563].

Poco tiempo después, los investigadores advirtieron que, si bien se comportaba como Petya, en realidad su objetivo no era obtener el pago de un rescate -de hecho, mostraba una dirección de bitcoin falsa-, sino dañar de forma irreparable los datos informáticos. En otras palabras, su objetivo era meramente destructivo. El Centro Criptológico Nacional de España resumió de forma clara cómo funcionaba este *malware*:

> El código dañino, pese a contar con características de *ransomware*, posee capacidades destructivas, ya que los sectores de arranque cifrados no pueden ser restaurados, incluso si se cumple una condición concreta los sectores del arranque son borrados en su totalidad impidiendo que el sistema operativo arranque. Del mismo modo, al haber cifrado archivos en el disco, estos no pueden ser recuperados excepto desde copias de seguridad previas[564].

Si bien el ataque inicialmente afectó compañías ucranianas, este *software* destructivo se diseminó globalmente y causó daños informáticos valorizados en diez mil millones de dólares. Por esta razón, es considerado como el ataque cibernético más costoso de la historia. Tanto Estados Unidos como la Unión Europea acusaron a un grupo de militares rusos de estar detrás de estas acciones[565].

Como el lector habrá notado, los ataques contra los datos informáticos pueden ser de distinta magnitud: desde afectar archivos electrónicos personales, generados por un usuario en un ámbito de investigación académica, hasta dañar miles de datos pertenecientes a una compañía como venganza por ser despedido o, incluso, ocasionar uno de los ataques más costosos de la historia de la informática, a nivel global y con fines posiblemente políticos.

---

563 Cludfare. *¿Qué son Petya y NotPetya?*, S/F. https://www.cloudflare.com/es-es/learning/security/ransomware/petya-notpetya-ransomware/

564 CCN-Cert. *Informe código dañino CCN-CERT ID 20/17. Código dañino .Petya/NotPetya*, publicado en julio del 2017, p. 5.

565 Tidy, Joe. *Rusia y Ucrania: los 3 ciberataques rusos que más teme Occidente*, publicado el 24 de marzo de 2022. https://www.bbc.com/mundo/noticias-60850173

6.2. REGULACIÓN EN EL CONVENIO SOBRE LA CIBERDELINCUENCIA

Bajo el nombre de *ataques a la integridad de los datos*, el artículo 4 del Convenio sobre la Ciberdelincuencia o Convenio de Budapest propone a los Estados sancionar esta conducta en los siguientes términos:

> **Art. 4.- Ataques a la integridad de los datos**
>
> 1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno todo acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos.
> 2. Las Partes podrán reservarse el derecho a exigir que los actos definidos en el párrafo 1 comporten daños graves.

La fórmula legislativa recomendada en el Convenio de Budapest puede graficarse de la siguiente forma:

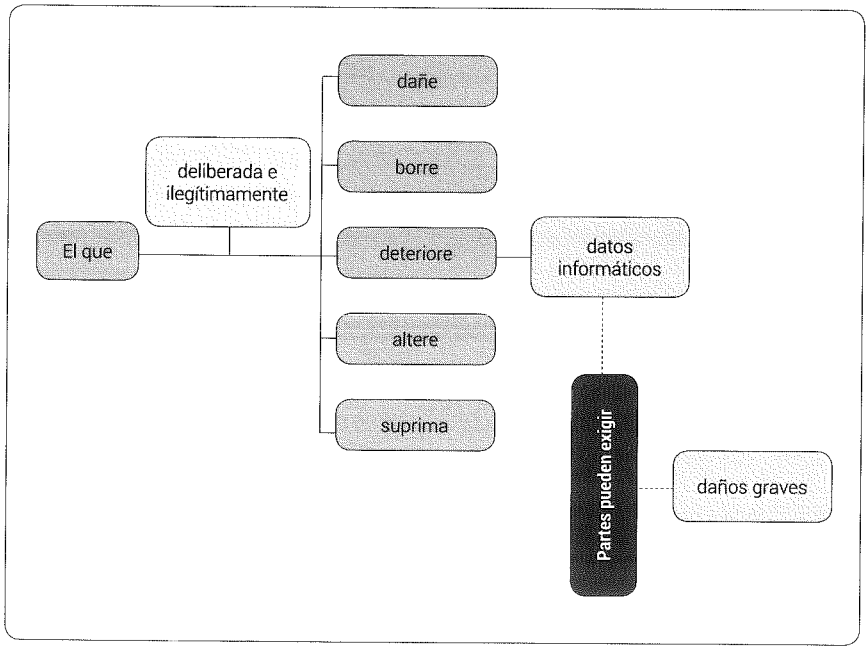


Diagrama 10. Estructura del delito de ataque a la integridad de los datos, propuesto en el Convenio de Budapest. Elaboración propia.

Los párrafos 60 a 64 del Informe Explicativo desarrollan el delito bajo análisis. A continuación, destacaré algunas ideas relevantes que permitirán comprender adecuadamente sus alcances e interpretación:

- En el párrafo 60, se precisa que la finalidad de esta disposición es proporcionar a los datos y a los programas informáticos una protección similar a los objetos corpóreos frente a ataques deliberados. Además, se indica que se busca tutelar la integridad y el correcto funcionamiento o utilización de los datos almacenados o de los programas informáticos. Esta precisión es importante, pues nos permitirá identificar el objeto de protección y, como más adelante señalaré, si bien la seguridad informática es el bien jurídico que se tutela, de manera general, la integridad y la disponibilidad es el interés central de esta norma -no así, la confidencialidad-.

- El párrafo 61 recoge las propuestas de definición de los cinco verbos rectores recogidos en el Convenio de Budapest: *dañar*, *deteriorar*, *borrar*, *suprimir* y *alterar*. Más adelante, se desarrollarán estos conceptos, compatibilizando su significado con el resto de verbos rectores; no obstante, en este punto, es importante indicar que la legislación peruana agrega algunas conductas adicionales: introducir y hacer inaccesible los datos informáticos.

  En este párrafo se indica, de modo ejemplificador, que "la introducción de códigos maliciosos, tales como virus y caballos de Troya, está incluido en este párrafo, tal como también lo está la modificación resultante de los datos".

- En el párrafo 62 se resalta que los actos deben ser ilegítimos, es decir, contrarios al ordenamiento -lo que, para nosotros, es antijurídico-. De este modo, los actos inherentes al diseño de las redes, las prácticas comerciales o de operación común no constituyen actos delictivos. Entre estas se enumeran: verificación o protección de la seguridad de un sistema informático autorizadas por el dueño o el operador, la reconfiguración del sistema operativo de un ordenador que tenga lugar cuando el operador de un sistema adquiere un nuevo *software*, la modificación de los datos relativos al tráfico con el fin de facilitar comunicaciones anónimas o la modificación de

datos con el fin de garantizar la seguridad de las comunicaciones (cifrado).

- El párrafo 63 recuerda que los actos ilícitos deben ser deliberados, es decir, dolosos. En el Perú, como más adelante veremos, se acuña este elemento también como parte de la tipicidad subjetiva exigida para la configuración del delito.
- Finalmente, en el párrafo 64 se recuerda que las partes pueden exigir que la conducta ilícita tenga como resultado un perjuicio grave. Nuestro país no hizo reserva sobre este punto.

6.3. REGULACIÓN EN LA CONVENCIÓN DE LAS NACIONES UNIDAS CONTRA LA CIBERDELINCUENCIA

Con un *nomen iurus* diferente, pero proponiendo tipificar la misma conducta, el artículo 9 de dicha convención recoge el delito de *interferencia con datos electrónicos* en los siguientes términos:

> **Art. 9.- Interferencia con datos electrónicos**
>
> 1. Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para tipificar como delito en su derecho interno todo acto deliberado y sin derecho que dañe, borre, deteriore, altere o suprima datos electrónicos.
> 2. Los Estados partes podrán exigir como requisito que los actos descritos en el párrafo 1 del presente artículo comporten daños graves.

La fórmula adoptada es afín al Convenio de Budapest. Así, de un lado, propone sancionar las mismas conductas: dañar, borrar, deteriorar, alterar o suprimir, y, de otro, faculta a los Estados a exigir que este comportamiento genere daños graves. Si bien, la Convención de las Naciones Unidas contra la Ciberdelincuencia no emplea la construcción lingüística *datos electrónicos* -como el Convenio de Budapest y la LDI-, la definición es idéntica: "Por datos electrónicos se entenderá toda representación de hechos, información o conceptos de una forma apta para el procesamiento mediante un sistema de tecnología de la información y las comunicaciones, incluido un programa adecuado para hacer que un sistema de tecnología de la información y las comunicaciones

ejecute una función" (art. 2 de la Convención de las Naciones Unidas contra la Ciberdelincuencia).

6.4. LEGISLACIÓN COMPARADA

El marco normativo adoptado por los diferentes países de la región latinoamericana permite sostener que es necesario homologar o uniformizar los verbos rectores previstos en este delito con la finalidad de minimizar la ambigüedad de algunos términos empleados y garantizar el principio de legalidad (*lex certa*). Algunos países, como Perú, incluyen modalidades no propuestas en el Convenio de Budapest sin que existan razones adecuadas que lo justifiquen.

País	Legislación	Tipo penal
Países latinoamericanos que se adhirieron al Convenio de Budapest		
Ecuador	**Código Orgánico Integral Penal**	Sección Tercera. Delitos contra la seguridad de los activos de los sistemas de la información y comunicación **Art. 232.- Ataque a la integridad de sistemas informáticos** La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento o comportamiento no deseado, o suprima total o parcialmente contenido digital [...], con el propósito de obstaculizar de forma grave, deliberada e ilegítima el funcionamiento de un sistema informático, será sancionada con pena privativa de libertad de tres a cinco años. **Art. 234.4 Definiciones** Para los efectos del presente Código, se considera: a. Contenido digital.- El contenido digital es todo dato informático que representa hechos, información o conceptos de la realidad, almacenados, procesados o transmitidos por cualquier medio tecnológico o canal de comunicación que se preste a tratamiento informático, incluidos los programas diseñados para un equipo tecnológico aislado, interconectado o relacionados entre sí.
Brasil	**Código Penal**	**Capítulo IV. Do dano** **Art. 163.- Dano** Destruir, inutilizar ou deteriorar coisa alheia: Pena - detenção, de um a seis meses, ou multa.
Colombia	**Código Penal**	**Título VII-A. De delitos contra el patrimonio cultural sumergido** **Art. 269 D.- Daño informático** El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos [...] incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.
Paraguay	**Código Penal**	**Capítulo II. Hechos punibles contra otros derechos patrimoniales** **Art. 174.- Alteración de datos** 1. El que lesionando el derecho de disposición de otro sobre datos los borrara, suprimiera, inutilizara o cambiara, será castigado con pena privativa de libertad de hasta dos años o con multa. 2. En estos casos, será castigada también la tentativa. 3. Como datos, en el sentido del inciso 1°, se entenderán sólo aquellos que sean almacenados o se transmitan electrónica o magnéticamente, o en otra forma no inmediatamente visible.

País	Legislación	Tipo penal
Argentina	Código Penal	**Capítulo VII. Daños** **Art. 183.-** Será reprimido con prisión de quince días a un año, el que destruyere, inutilizare, hiciere desaparecer o de cualquier modo dañare una cosa mueble o inmueble o un animal, total o parcialmente ajeno, siempre que el hecho no constituya otro delito más severamente penado. En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas [...].
Costa Rica	Código Penal	**Sección VII. Daños** **Art. 229 bis.- Daño informático** Se impondrá pena de prisión de uno a tres años al que sin autorización del titular o excediendo la que se le hubiera concedido y en perjuicio de un tercero, suprima, modifique o destruya la información contenida en un sistema o red informática o telemática, o en contenedores electrónicos, ópticos o magnéticos. La pena será de tres a seis años de prisión, si la información suprimida, modificada, destruida es insustituible o irrecuperable.
Chile	Ley N.° 21459	**Título I. De los delitos informáticos y sus sanciones** **Art. 4.- Ataque a la integridad de los datos informáticos** El que indebidamente altere, dañe o suprima datos informáticos, será castigado con presidio menor en su grado medio, siempre que con ello se cause un daño grave al titular de estos mismos.
Panamá	Código Penal	**Capítulo I. Falsificación de documentos en general** **Art. 366-A.** Quien indebidamente ingrese, altere, borre, suprima o falsifique datos informáticos, un documento electrónico, un certificado electrónico independientemente de si los datos pueden o no ser leídos directamente o almacenados en un sistema informático o electrónico resultando en datos informáticos no auténticos para que sean adquiridos o utilizados como auténticos con efectos legales, será sancionado con prisión de cuatro a ocho años.
República Dominicana	Ley N.° 53-07	**Capítulo I. Crímenes y delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos** **Art. 10.- Daño o Alteración de Datos** El hecho de borrar, afectar, introducir, copiar, mutilar, editar, alterar o eliminar datos y componentes presentes en sistemas electrónicos, informáticos, telemáticos, o de telecomunicaciones, o transmitidos a través de uno de éstos, con fines fraudulentos, se sancionará con penas de tres meses a un año de prisión y multa desde tres hasta quinientas veces el salario mínimo. Párrafo.- Cuando este hecho sea realizado por un empleado, exempleado o una persona que preste servicios directa o indirectamente a la persona física o jurídica afectada, las penas se elevarán desde uno a tres años de prisión y multa desde seis hasta quinientas veces el salario mínimo.
Otras referencias		
España	Código Penal	**Capítulo IX. De los daños** **Art. 264.** 1. El que por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a tres años. 2. Se impondrá una pena de prisión de dos a cinco años y multa del tanto al décuplo del perjuicio ocasionado, cuando en las conductas descritas concurra alguna de las siguientes circunstancias: 1.ª Se hubiese cometido en el marco de una organización criminal. 2.ª Haya ocasionado daños de especial gravedad o afectado a un número elevado de sistemas informáticos. 3.ª El hecho hubiera perjudicado gravemente el funcionamiento de servicios públicos esenciales o la provisión de bienes de primera necesidad.

País	Legislación	Tipo penal
España	Código Penal	4.ª Los hechos hayan afectado al sistema informático de una infraestructura crítica o se hubiera creado una situación de peligro grave para la seguridad del Estado, de la Unión Europea o de un Estado Miembro de la Unión Europea. A estos efectos se considerará infraestructura crítica un elemento, sistema o parte de este que sea esencial para el mantenimiento de funciones vitales de la sociedad, la salud, la seguridad, la protección y el bienestar económico y social de la población cuya perturbación o destrucción tendría un impacto significativo al no poder mantener sus funciones. 5.ª El delito se haya cometido utilizando alguno de los medios a que se refiere el artículo 264 ter. Si los hechos hubieran resultado de extrema gravedad, podrá imponerse la pena superior en grado. 3. Las penas previstas en los apartados anteriores se impondrán, en sus respectivos casos, en su mitad superior, cuando los hechos se hubieran cometido mediante la utilización ilícita de datos personales de otra persona para facilitarse el acceso al sistema informático o para ganarse la confianza de un tercero.

Cuadro 19. Legislación comparada respecto al delito de atentado a la integridad de datos informáticos. Elaboración propia.

La legislación penal analizada ubica este ilícito, principalmente, en el capítulo de delitos contra el patrimonio o daños (Argentina, Brasil, Colombia, Costa Rica, España y Paraguay). Sin embargo, algunas legislaciones también lo sitúan en el capítulo de delitos contra la seguridad informática (Ecuador y República Dominicana) o de los delitos informáticos (Chile).

Algunos países (Argentina, Colombia, Ecuador) han unido en un solo artículo el delito de atentado contra los datos informáticos y el delito de atentado contra los sistemas informáticos. El resto de los países los tipifica de forma independiente y, en algunos casos, diferencian el *quantum* de la pena.

A diferencia del acceso ilícito en el que el *nomen iuris* es idéntico en las legislaciones analizadas, este delito recoge diferentes denominaciones: *daño informático* (Colombia y Costa Rica), *alteración de datos* (Paraguay), *ataque a la integridad de los datos informáticos* (Chile) y *daño o alteración de datos* (República Dominicana).

Es importante resaltar que ordenamientos comparados como el chileno y el español exigen que el delito analizado ocasione un significativo perjuicio. Así, el artículo 264 del Código Penal español sanciona a quien "por cualquier medio, sin autorización y **de manera grave** borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesible datos informáticos, programas informáticos o documentos electrónicos ajenos, cuando el **resultado producido fuera grave** [...]". En esta línea, la doctrina hispana concluye que, en su legislación, tanto el

ataque como el resultado deben ser graves[566] -"concepto indeterminado que debe evaluarse conforme a la potencialidad lesiva que la conducta presenta, lo que a su vez depende tanto de su probabilidad de éxito como del valor y la utilidad de los datos, programas o documentos y la disminución de la funcionalidad y utilidad del sistema que pueda provocar. Además, para que se consume el delito es preciso no solo que la conducta presente ex ante esta peligrosidad grave (lo que bastaría para condenar por tentativa), sino, además, haber causado efectivamente un resultado grave. La gravedad del resultado se medirá de la misma manera, atendiendo conjuntamente al valor y la utilidad de los elementos borrados, dañados, etc., y a las consecuencias que la conducta ha producido para la propia funcionalidad del sistema y su utilidad para su titular"[567]-.

Entre los verbos rectores que no se consideran adecuados, según tanto el Convenio como la Convención, figuran los siguientes: *destruir*, *inutilizar*, *cambiar*, *modificar*, *afectar*, *introducir*, *copiar*, *mutilar*, *editar*, *eliminar*, *hacer inaccesible*. Agregar estos verbos rectores, sin mayor justificación, genera problemas al definirlos e interpretar sus alcances.

Finalmente, el objeto sobre el cual recae la acción adopta diferentes denominaciones: *contenido digital*, *información*, *datos*, *datos informáticos*, *documento electrónico*, *certificados electrónicos*, *programas informáticos*, *componentes de sistemas informáticos*. Al igual que en la recomendación anterior, sería bueno uniformizar el objeto de protección pudiendo tomar como marco de referencia el Convenio de Budapest (datos informáticos) o la Convención de las Naciones Unidas contra la Ciberdelincuencia (datos electrónicos).

6.5. LEGISLACIÓN NACIONAL

Al igual que el delito de acceso ilícito, los daños informáticos fueron incorporados al ordenamiento penal peruano en el año 2000, aunque su formulación inicial dista considerablemente de la regulación vigente. En las líneas que siguen, se presenta un breve recorrido histórico que nos conduce hasta la normativa actual, en la cual nos detendremos para analizar el tipo penal vigente.

566 Velasco Núñez, Eloy y Carolina Sanchís Crespo. *Delincuencia informática. Tipos delictivos e investigación. Con jurisprudencia tras la reforma procesal y penal del 2015*. Valencia: Tirant lo Blanch, 2019, p. 51.

567 Gil Gil/Hernández Berlinches, *Cibercriminalidad*, cit., p. 216.

6.5.1. Antecedentes normativos

Dos proyectos de ley, presentados en 1999, fueron la base para la incorporación del delito de daño de datos informáticos en nuestro Código Penal.

- **Proyecto de Ley N.º 5071/99-CR**, presentado el 18 de agosto de 1999 por el congresista Jorge Muñiz Ziches[568]. Este proyecto incorpora el elemento *indebidamente* en el tipo penal y, además, propone tres conductas típicas: *alterar*, *dañar* o *destruir*.
- **Proyecto de Ley N.º 5132/99-CR**, presentado el 31 de agosto de 1999 por la congresista Susana Díaz Díaz[569]. A diferencia del proyecto anterior, este sugiere la creación de una ley especial y recomienda sancionar las conductas cometidas de forma maliciosa -sugerencia que no prosperaría-. No obstante, el elemento "datos contenidos en un sistema de tratamiento de información" sería el antecedente de lo que se conocería, más adelante, como dato informático.

La autógrafa remitida al Ejecutivo fue observada. Poco tiempo después, el 14 de junio de 2000, se recibió un dictamen por unanimidad de la Comisión de Reforma de Códigos en el que se incluyeron algunos comentarios muy interesantes:

> El ámbito del injusto penal del artículo 208-B prevé las acciones que atentan contra la integridad de los elementos informáticos, que es el caso del vandalismo o terrorismo informático cuya finalidad primaria es causar perjuicio. Sin embargo, es importante recalcar que la configuración de este tipo penal responde también a un delito de peligro en la que no es necesario comprobar la afectación del bien jurídico tutelado, pues se busca establecer que el propio ánimo de alterar o destruir o interferir en el programa o en el sistema o red de computadoras con-

568 **Proyecto de Ley N.º 5071/99-CR, art. 209-B.-** El que indebidamente, [...] altere, dañe o destruya un soporte o programa de computadora o los datos contenidos en la misma, en la base, [...] será reprimido con pena privativa de la libertad no mayor de dos años.

569 **Proyecto de Ley N.º 5132/99-CR, art. 3.-** El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será sancionado con pena privativa de libertad no mayor de cuatro años.

> figure ya este delito, debido a que el modo de perpetración del mismo es uno que no deja rastro de su comisión.

El 21 de junio de 2000, se debatió el proyecto sustitutorio, aprobándose el siguiente texto, que se encontró vigente hasta octubre del 2013, fecha en el que entró en vigor la LDI:

> **Art. 207-B CP.- Alteración, daño y destrucción de base de datos, sistema, red o programa de computadoras.** El que utiliza, ingresa o interfiere indebidamente una base de datos [...] o programa de computadoras o cualquier parte de la misma con el fin de alterarlos, dañarlos o destruirlos, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años y con setenta a noventa días multa.

6.5.2. Génesis legislativa

De los ocho proyectos de ley que dieron origen a la promulgación de la LDI, este delito tomó como base dos de ellos:

- **Proyecto de Ley N.º 00034/2011-CR**, presentado el 11 de agosto de 2011 por el congresista Juan Carlos Eguren Neuenschwander[570]. El tipo penal propuesto (i) recogía cuatro verbos rectores, a diferencia de los ocho que actualmente se sancionan: *destruir*, *dañar*, *modificar* o *inutilizar*; (ii) no empleó la construcción lingüística *datos informáticos*, sino la voz *data*, ampliándose el objeto de tutela a la información contenida en sistemas de información, tecnologías de información o sus componentes.
- **Proyecto de Ley N.º 2520/2012-PE**, presentado el 26 de julio de 2013 por el presidente de la República Ollanta Humala Tasso[571].

---

570 **Proyecto de Ley N.º 00034/2011-CR, art. 4.-** ***Sabotaje informático.*** [...] Se le impondrá la misma pena a quien destruya, dañe, modifique o inutilice la data o la información contenida en cualquier sistema de información o tecnología de información o en cualquiera de sus componentes.

571 **Proyecto de Ley N.º 2520/2012-PE, art. 208-B-** ***Atentado a la integridad de datos informáticos.*** El que, a través de las tecnologías de la información o de la comunicación, introduce, borra, deteriora, altera, suprime, o hace inaccesibles datos informáticos será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa.

Esta propuesta es la más cercana al tipo penal aprobado. En este caso, (i) se sugirió sancionar cinco conductas: *introducir, borrar, deteriorar, alterar, suprimir* o *hacer inaccesible*; (ii) se estableció que el objeto material del delito es el *dato informático* -siguiendo el Convenio de Budapest-; (iii) se precisó que el medio comisivo son las TIC, elemento que se recogió en el delito inicialmente aprobado.

6.5.3. Evolución legislativa

Como se ha señalado en capítulos precedentes, tan solo bastaron cinco meses para que la LDI sufriera cambios estructurales en su configuración. En lo que se refiere a este delito, su modificación fue propuesta en dos proyectos legislativos:

- **Proyecto de Ley N.º 02991/2013**, presentado el 25 de noviembre de 2013 por el congresista Juan Carlos Neuenschwander[572]. Esta propuesta incorporó los elementos *deliberada* e *ilegítimamente*, previstos en el Convenio de Budapest, pero que devienen en innecesarios, ya que nuestro ordenamiento exige que la conducta sea dolosa e ilegítima. Además, este proyecto es el que recomienda agregar una conducta típica adicional: *introducir*. El Convenio de Budapest no recomienda este verbo rector sino al regular el delito de sabotaje informático -que será analizado en el siguiente capítulo-.
- **Proyecto de Ley N.º 02999/2013**, presentado el 27 de noviembre de 2013 por el congresista Mauricio Mulder Bedoya[573]. Al igual que en el caso anterior, se propone incorporar los elementos *deliberada* e *ilegítimamente*, pero no sugiere agregar o eliminar verbo rector alguno.

572 **Proyectos de Ley N.º 02991/2013, art. 3. *Atentado a la integridad de datos informáticos.*** El que deliberada e ilegítimamente daña, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa.

573 **Proyecto de Ley N.º 02999/2013, art. 3. *Atentando a la integridad de datos informáticos.*** El que de manera deliberada e ilegítima, dañe, borre, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa.

6.5.4. Regulación actual

El siguiente cuadro permite comparar los cambios normativos del delito de atentado contra la integridad de datos informáticos y conocer su actual regulación:

Art. 3 LDI (Original)	Art. 3 LDI (Actual)
Ley N.° 30096	Modificado por la Ley N.° 30171
El que, a través de las tecnologías de la información o de la comunicación, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa.	El que deliberada e ilegítimamente daña, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa.

Cuadro 20. Regulación del delito de atentado contra la integridad de datos informáticos, 2013-2024. Elaboración propia.

En Perú, a diferencia de la legislación comparada, el delito de atentado contra la integridad de los datos informáticos no exige *gravedad* alguna. Esta opción legislativa se aparta de la política criminal que orienta la lucha contra otros delitos. Así, en atención al valor económico del bien, en el hurto y en el daño, nuestro ordenamiento penal sí distingue entre delito (arts. 185 y 205 CP) y falta (art. 444 CP). Lo mismo sucede con la gravedad de las lesiones (arts. 122 y 441 CP) o la extensión temporal de la usurpación (arts. 202 y 446 CP).

En el delito bajo análisis, no se ha previsto esta distinción y, en consecuencia, la gravedad no es un elemento objetivo del tipo; sin embargo, sí debería recogerse este elemento para evitar criminalizar daños informáticos poco lesivos, esto es, analizar y excluir supuestos de mínima lesividad[574].

Ahora bien, si comparamos el Convenio de Budapest, la Convención de las Naciones Unidas contra la Ciberdelincuencia y la legislación penal local, apreciamos que el legislador peruano incluyó todos los verbos rectores sugeridos en el Convenio de Budapest, pero, agregó dos acciones típicas adicionales: *in-*

574 En el mismo sentido: "[...] la descripción legal tampoco ofrece los criterios necesarios para excluir de la tutela penal aquellos supuestos de mínima lesividad, por ejemplo, la mínima permanencia o afectación a la integridad de datos o sistemas. En este supuesto, mediante una reforma se podría brindar las pautas necesarias para discernir los casos menos graves, comportamientos que podrían considerarse circunstancias de atenuación" (Requejo Passoni, "Avances y retrocesos de la política criminal relativa a los delitos contra datos y sistemas informáticos en el Perú", cit., p. 52).

troducir y *hacer inaccesible*. Como veremos más adelante, esta inclusión genera problemas de interpretación.

	Convenio de Budapest	Convención de las Naciones Unidas contra la Ciberdelincuencia	Ley de Delitos Informáticos
	Ataques a la integridad de los datos (art. 4)	Interferencia con datos electrónicos (art. 9)	Atentado a la integridad de datos informáticos (art. 3)
Dañar	X	X	X
Borrar	X	X	X
Deteriorar	X	X	X
Alterar	X	X	X
Suprimir	X	X	X
Introducir	-	-	X
Hace inaccesible	-	-	X

Cuadro 21. Comparación de los verbos rectores recogidos en el artículo 4 del Convenio de Budapest, el artículo 9 de la Convención de las Naciones Unidas contra la Ciberdelincuencia y en el artículo 3 de la LDI. Elaboración propia.

La actual tipificación del delito de atentado contra la integridad de datos informáticos en la legislación penal peruana recoge la siguiente configuración:

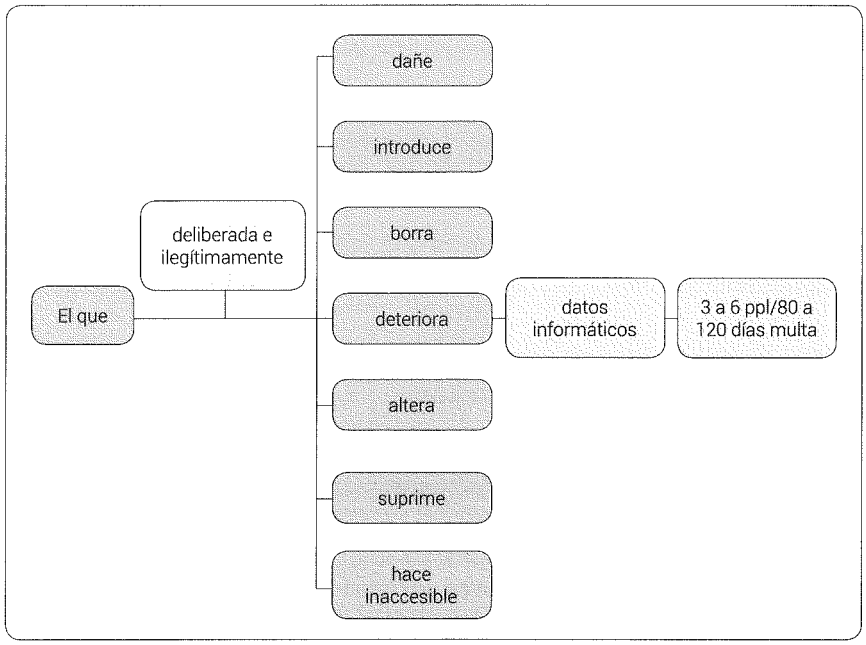


Diagrama 11. Estructura actual del delito de atentado contra la integridad de datos informáticos, en el sistema penal peruano. Elaboración propia.

6.6. EL BIEN JURÍDICO PENALMENTE PROTEGIDO

Algunas legislaciones ubican este ilícito en el capítulo de los delitos contra el patrimonio, lo que ha orillado a cierto sector de la doctrina a considerar que el bien jurídico protegido es el caudal económico o el patrimonio, valga la redundancia. Aun en dichos escenarios, se reconoce que la protección no debe ser únicamente económica. Por esta razón, se advierte que nos encontramos frente a un nuevo bien jurídico:

> Como hemos dicho anteriormente, los delitos informáticos regulados en el título correspondiente a las infracciones contra la propiedad abarcan algo más que la relación de disposición sobre los datos en un sentido económico del término. También la integridad y la funcionalidad de los sistemas o programas informáticos son tenidos debidamente en cuenta por el legislador al momento de describir el sentido y el alcance de la conducta prohibida. En particular, como lo señala correctamente la doctrina, los datos objeto de agresión por la conducta del autor pueden ser o no de naturaleza económica, lo que refleja la importancia de analizar de manera adecuada el ámbito de protección de esta norma penal en particular. El delito de daño informático aquí analizado está orientado de manera prudente hacia la propia integridad y funcionalidad del sistema informático en su conjunto, es decir, como expresión de la libertad de disposición de estos datos en el ejercicio de la autodeterminación informativa[575].

En Argentina, el delito analizado se encuentra en el Libro II, Título VI, destinado a la protección del bien jurídico *propiedad*. Algunos autores resaltan la reforma de la Ley N.º 26388, pues extendió la protección jurídico-penal a los bienes intangibles: datos, documentos, programas y sistemas informáticos[576].

En España, este delito se ubica en el capítulo IX, denominado *De los daños*, e integra el título XIII del Código Penal que sanciona los *Delitos contra el patrimonio y el orden socioeconómico*. No obstante, se sostiene que este tipo

575 Aboso, *Derecho penal cibernético*, cit., p. 356.

576 Kiefer, Mariana. "Daño informático". En: Dupuy, Daniela (dir.) y Mariana Kiefer (coord.) *Cibercrimen. Aspectos de derecho penal y procesal penal. Cooperación internacional. Recolección de evidencia digital. Responsabilidad de los proveedores de servicios de Internet*. Montevideo: B de F, 2019, p. 327.

de delitos no solo protegen los derechos materiales del titular, sino también la información contenida. Entonces, "por todo ello, se produce una despatrimonialización de la concepción tradicional que debería llevar aparejada una ubicación distinta, naturalmente autónoma para el *cracking*"[577].

En Colombia, el artículo 269D de su Código Penal sanciona tanto las conductas dirigidas contra los datos como contra los sistemas informáticos y sus componentes físicos (*hardware*). Por esta razón, en dicho país, autores como Ricardo Posada Maya sostienen que es un delito pluriofensivo e implica una lesión de la seguridad de la información, en particular de la integridad, aplicabilidad y disponibilidad de los datos, los sistemas y sus partes y componentes lógicos. No obstante, reconoce que, además, al tutelarse los componentes físicos, se protege de manera secundaria el patrimonio económico[578].

A nivel local, Víctor Espinoza considera que este delito tutela la ciberseguridad e intangibilidad de la información e, incluso, el patrimonio digital, "entendido como la información que posee cada sistema informático"[579]. Coincido con su postura si es que se equipara la ciberseguridad con la seguridad informática, pero no con la protección de la información, ya que se tutela una manifestación específica: los datos informáticos. Tampoco considero adecuado sostener que el patrimonio digital es el bien jurídico protegido, ya que podría interpretarse como un delito contra el patrimonio, cuando no lo es. Aunque los datos informáticos posean un valor en el mercado o para el usuario, eso no significa que se proteja el patrimonio.

De otro lado, Vega Aguilar y Arévalo Minchola consideran que no se protege el patrimonio, sino la integridad informática, "entendiendo a esta como el conjunto de datos informáticos que se destruyen, inutilizan, dañan y/o modifican con la acción del ciberdelincuente"[580]. En la misma línea, Pérez

577 Barrio Andrés, *Delitos 2.0. Aspectos penales, procesales y de seguridad de los ciberdelitos*, cit., p. 108. De otro lado, en México, cierto sector considera que "el bien jurídico protegido en cuestión sería la protección de la información". Montoya Piña, Javier Omar. *Delitos federales cometidos a través de medios informáticos*. México D.F.: Flores Editores y Distribuidores, 2015, p. 86.

578 Posada Maya, *Los cibercrímenes*, cit., p. 349.

579 Espinoza Calderón, *Delitos informáticos y nuevas modalidades delictivas*, cit., p. 76.

580 Arévalo Minchola/Vega Aguilar, *Ciberdelitos. Análisis en el sistema penal*, cit., p. 271.

López señala que el patrimonio no es el objeto de tutela, sino "la seguridad e intangibilidad del tráfico de información en la red"[581]. Coincido con estas posiciones, sin embargo, además de la integridad, también se tutela la disponibilidad informática, como más adelante se explicará.

Meneses Gonzáles y Meneses Ochoa tienen una posición mucho más amplia, pues sostienen que se tutela "la integridad, intangibilidad, disponibilidad y el correcto funcionamiento de los datos informáticos"[582].

En esta obra, sostengo que el delito de daños informáticos protege la seguridad informática -de manera general-, así como su integridad y disponibilidad -de forma particular-, en este caso entendida como el correcto funcionamiento o utilización de los datos y programas informáticos, tal y como precisa el Informe Explicativo antes mencionado: "La finalidad de esta disposición es proporcionar a los datos informáticos y a los programas informáticos una protección similar a la que gozan los objetos corpóreos contra la imposición de un daño deliberado"[583]. Esta interpretación es adecuada, pues, de un lado, un programa es un conjunto de datos informáticos que constituyen una secuencia de instrucciones para realizar una labor específica. De otro, impide que se genere un vacío de protección penal. De ello se desprende que el objeto de protección no es la confidencialidad de los datos informáticos -protegido por los delitos de acceso ilícito y de interceptación ilegal-.

6.7. TIPICIDAD OBJETIVA

6.7.1. Sujetos

Es un delito común. El sujeto activo puede ser cualquier persona que atente contra la integridad o disponibilidad de los datos informáticos, sin que se exija una condición cualificada o, incluso, sin que ostente conocimientos técnicos especializados.

581 Pérez López, *Delitos regulados en leyes penales especiales*, cit., p. 116.

582 Meneses Gonzáles/Meneses Ochoa, *La cibercriminalidad: Consideración criminológica, político-criminal, dogmática, procesal y cooperación internacional*, cit., p. 311.

583 Parágrafo 60 del Informe Explicativo.

Para algunos autores, si bien cualquier persona puede cometer este delito, el sujeto activo "es siempre una persona con conocimientos promedios o avanzados, ya que se requiere cierto conocimiento especializado en informática"[584]. En similar posición, se sostiene que "en este delito y en todos los demás delitos informáticos, se exige que el sujeto activo sea aquella persona que tenga las condiciones técnicas suficientes para poder manipular la informática y así cometer algún delito informático. En otras palabras, no va a ser cualquier persona, sino cualquiera que se encuentre dentro de la clasificación del delincuente informático, pero quienes cometen este tipo de delitos son los *crackers* y los *viruckers*"[585].

Discrepo de esta posición, porque las herramientas técnicas pueden ser adquiridas fácilmente, por ejemplo, en la *dark web*[586], en redes sociales o, incluso, en espacios físicos como el Centro de Lima[587]. Es más, hasta en YouTube existen tutoriales que explican con mucha facilidad -para quien no tiene conocimiento técnico alguno- cómo cometer este tipo de delitos. Ahora bien, este delito sanciona, incluso, al empleado que, sin autorización alguna, modifica los archivos informáticos de su institución, lo que no exige mayor pericia o destreza.

---

584 Espinoza Calderón, *Delitos informáticos y nuevas modalidades delictivas*, cit., p. 78.

585 Jiménez Herrera, *Manual de derecho penal informático*, cit., p. 412.

586 "Existen redes informáticas a las cuales solo pueden acceder determinadas personas y utilizando ciertos soportes del ciberespacio. Se trata de actividades en la Internet Profunda o Darknet, que solamente están disponible para quienes tengan acceso a un espacio encriptado y ocultando que sirve para realizar acciones prohibidas e ilícitas, difícilmente rastreables por alguien que no tenga conocimientos especiales y las herramientas adecuadas. En este sentido, la Darnet contiene información de acceso mucho más fácil de manejar para un hacker, que podrá cometer ciberestafas, piratería informática, ciber-espionaje, tráfico de armas, drogas o de personas, etc. Y claro, los problemas se producen al existir una amplia variedad de delitos que se realizan cada vez con más frecuencia en el ciberespacio con una difícil y pronta persecución penal especialmente por la difícil geolocalización del ciberdelincuente" (Verdugo Guzmán, Silvia Irene. "Cibercrimen, internet oscura y COVID-19. Inteligencia artificial y transformación digital". En: Madrid Parra, Agustín y Lucía Alvarado Herrera [dirs.]. *Derecho digital y nuevas tecnologías*. Navarra: Thomson Reuters / Aranzadi, 2022, pp. 981 y s).

587 Recomiendo el reportaje de *El Comercio*. "Desde venta de placas madre hasta billetes falsos y mascotas sin control: los negocios ilícitos del Cercado de Lima", en *El Comercio*, 27 de febrero de 2025. https://elcomercio.pe/lima/policiales/los-negocios-ilicitos-del-cercado-de-lima-desde-venta-de-placas-madre-hasta-billetes-falsos-y-mascotas-sin-control-policiales-noticia/

El sujeto pasivo puede ser cualquier persona, sea natural o jurídica. Para Jiménez Herrera, "el sujeto pasivo será aquel que ejerce la titularidad sobre la información contenida en el dato informático; sin embargo, también puede ser aquel quien ejerce la administración o responsabilidad de los datos informáticos"[588]. De este modo, para el autor mencionado, en este tipo penal se diferencia un sujeto pasivo del delito (titular del bien jurídico) y el sujeto pasivo de la acción (responsable del bien jurídico).

En mi opinión, el sujeto pasivo es el titular de los datos informáticos dañados[589].

Se sostiene que existe una cifra negra en los delitos contra la seguridad informática, es decir, que la cantidad de casos denunciados es significativamente menor que la cantidad real de hechos delictivos. Esta situación es una característica común en este tipo de delitos, debido al elevado número de víctimas que generan:

> Este tipo de delitos se caracterizan por la dificultad para descubrirlos y derivado de esto su probación y persecución, motivo por el cual no se denuncian por el sujeto pasivo, lo que agrava el conocimiento de las autoridades en las cifras de este tipo de delitos y por lo tanto la no adecuada planificación de medidas preventivas y sancionadoras a tales acciones ilícitas, aunado a esto contribuye la falta de preparación por parte de las autoridades, todo lo anterior trae como consecuencia que las estadísticas sobre este tipo de conductas contribuya a la denominada cifra negra[590].

6.7.2. Acciones típicas

Es importante analizar los verbos rectores que se recogen en nuestro país para comprender la necesidad de su modificación. Así, sin mayor explicación o debate, el legislador peruano no solo tomó como referencia los cinco verbos

588 Jiménez Herrera, *Manual de derecho penal informático*, cit., p. 412.

589 En esta línea, Barrio Andrés, *Delitos 2.0. Aspectos penales, procesales y de seguridad de los ciberdelitos*, cit., p. 109.

590 Montoya Piña, *Delitos federales cometidos a través de medios informáticos*, cit., pp. 90 y s.

rectores sugeridos en el Convenio de Budapest, sino que agregó dos más: *introducir* y *hacer inaccesible* los datos informáticos.

Debe tenerse presente que el origen de los verbos rectores *introducir* y *hacer inaccesibles* no proviene del Convenio sobre la Ciberdelincuencia, sino que se remonta al proyecto de Ley N.º 2520/2012, propuesto por el presidente Ollanta Humala. Lastimosamente, la exposición de motivos no desarrolla estos conceptos, sino que se limita a sostener lo siguiente: "En el delito de atentados a la integridad de datos informáticos se tipifica las conductas consistentes en afectar de diversas formas (borrar, alterar, suprimir, etc.) datos informáticos". Por esta razón, toda interpretación que se efectúe debe tomar como punto de partida los conceptos previamente descritos y, así, evitar contradicciones.

Ahora bien, en el fundamento jurídico 4.6 del Recurso de Nulidad N.º 743-2018, Lima, del 26 de octubre de 2018, la Sala Penal Permanente de la Corte Suprema de Justicia de la República recordó que "la redacción del tipo penal de atentado contra la integridad de datos informáticos contempla varios verbos rectores como introducir, borrar, deteriorar, alterar y/o suprimir datos informáticos falsos". De ahí que, en algunos casos, nos encontremos frente a supuestos concursales, ya que el mismo hecho no puede generar dos conductas diferentes. Dicho esto, será muy importante diferenciar los alcances de cada verbo rector.

En nuestro país, al igual que en otras latitudes, si bien se recogen diversos verbos rectores se debe tomar en consideración que el resultado producido como consecuencia de una u otra acción no revisten el mismo nivel, intensidad o gravedad. En tal sentido, se sostiene que constituyen diversos grados de desvalor de acción y resultado:

> En efecto, de cara al principio de lesividad [...] no resulta lo mismo destruir un sistema informático que inutilizarlo. Por lo que concierne al desvalor de acción, tampoco parece adecuado afirmar -a priori- una mayor gravedad del delito cuando el daño (destrucción, inutilización, desaparecimiento o daño de cualquier otro modo) sea realizado por medio de la fuerza física que por la violencia informática; entre otras cosas, porque no es cierto que la segunda modalidad (la informática) constituya una forma menos peligrosa de lesionar o colocar en peligro el bien jurídico tutelado en comparación con la primera, y porque el

> criterio para graduar el desvalor de acción no depende exclusivamente de la mayor o menor cantidad de movimientos corporales naturalísticos que realice el agente con dolo de dañar los bienes protegidos. De este modo, con un simple "click" se puede realizar una conducta más lesiva de inutilización que aquella producida por actividades de naturaleza física. Ello demuestra la necesidad de distinguir los diversos grados de desvalor de acción y resultado que tales verbos rectores sobrellevan, o precisar un criterio de individualización de la pena más preciso respecto de los delitos de daño en bien ajeno, sobre todo cuando su desarrollo implique utilizar medios informáticos que afecten los equipos físicos[591].

A continuación, propondré definiciones que compatibilicen cada uno de los verbos rectores recogidos en la LDI. Para ello, empleo el siguiente esquema de trabajo:

- Se coloca a pie de página la definición prevista en el diccionario de la Real Academia de la Lengua Española.
- Al costado del verbo rector colocaré la voz original en inglés, ya que es el idioma oficial del Convenio de Budapest[592].
- Se coloca también a pie de página la definición de la voz en inglés.
- En algunos casos, se utiliza doctrina comparada si es que el verbo rector se encuentra previsto en la legislación estudiada.
- Se citan estudios nacionales para establecer algunos puntos comunes.
- En ciertos casos, se transcribe la definición propuesta en el Informe Explicativo.
- Se utilizan algunos ejemplos o casos que permiten explicar los alcances del verbo rector estudiado.
- Finalmente, expongo mi propuesta de definición.

591 Posada Maya, *Los cibercrímenes*, cit., p. 357.

592 Las acepciones recogidas a continuación han sido tomadas del diccionario de la Real Academia Española y del *Oxford Advanced Learners's Dictionary*.

6.7.2.1. Dañar[593], *damaging*[594]

A nivel comparado, Colombia, Chile y España recogen expresamente esta conducta.

Dañar datos informáticos fue incorporado a nuestra legislación por la Ley N.º 30171 de marzo del 2014 y tiene como antecedente el proyecto de Ley N.º 3105/2013 del grupo parlamentario Perú Posible. Lamentablemente, la propuesta normativa no explicó ni justificó la necesidad de su incorporación.

En Colombia, con las acotaciones dadas previamente sobre la construcción típica de este delito, se sostiene que *dañar* es "causar detrimento, perjuicio o menoscabo negativo o lógico, en la integridad total o parcial, permanente o temporal de los datos, sistemas informáticos, partes o componentes lógicos, o en el contenido de estos. Es un verbo rector general que cubre el sentido típico de los otros verbos concurrentes, pues al fin de cuentas todos son formas de daño o menoscabo"[595].

Son pocos los autores locales que definen este verbo. Para Espinoza Calderón, significa "causar perjuicio a los datos informáticos, el daño puede ser reversible o irreversible dependiendo de su magnitud"[596], mientras que para Vega Aguilar y Arévalo Minchola, "esta modalidad se estaría presentando cuando el sujeto agente menoscaba o causa perjuicio a un determinado dato informático"[597]. De similar parecer es Pérez López, quien sostiene que esta modalidad se configura cuando "el agente dolosamente menoscaba, causa detrimento, perjudica, estropea o deteriora una base de datos que total o parcialmente corresponde a otra persona que viene a ser el sujeto pasivo de la acción. Consiste en disminuir el valor patrimonial de la base de datos, comprometiendo fundamentalmente el aspecto corporal o material con el que está elaborado o hecho, sin que represente su inutilización. Lo único que busca el autor es deteriorarlo para que no siga cumpliendo su normal finalidad, es decir, mermar su funcionamiento"[598].

---

593 Causar detrimento, perjuicio, menoscabo, dolor o molestia.

594 Causing damage; having a bad effect on someone or something.

595 Posada Maya, *Los cibercrímenes*, cit., p. 353.

596 Espinoza Calderón, *Delitos informáticos y nuevas modalidades delictivas*, cit., p. 77.

597 Arévalo Minchola/Vega Aguilar, *Ciberdelitos. Análisis en el sistema penal*, cit., p. 273.

598 Pérez López, *Delitos regulados en leyes penales especiales*, cit., pp. 116 y s.

En esta línea, el parágrafo 61 del Informe Explicativo indica que "los términos que dañe y deteriore como actos imbricados se refieren en particular a una alteración negativa de la integridad o del contenido de la información de los datos y programas".

Sugiero que el verbo *dañar* debe entenderse como una conducta de carácter residual, es decir, si el atentado contra la integridad de los datos informáticos no se subsume en ninguna de las siete modalidades, puede tener cobertura bajo este verbo rector, ya que *dañar* significa causar detrimento, perjuicio o menoscabo, de forma general.

6.7.2.2. Introducir[599]

A nivel comparado, solo República Dominicana recoge este verbo.

Entre las definiciones peruanas de este verbo encontramos: "Agregar o adicionar datos e información que no estaba inicialmente"[600], "hacer que una cosa ingrese total o parcialmente en el interior de otra; y en el caso específico se trataría de hacer ingresar alguna información al interior de datos informáticos"[601] y "acción de agregar nuevos datos sistemáticos a un conjunto de información existente"[602]. En el ámbito local, Pérez López critica que se haya incluido este verbo rector ya que carece de sentido y atenta contra el principio de lesividad[603] -posición que comparto-.

En este caso, a diferencia del resto de conductas, se castiga a quien deliberada e ilegítimamente agrega datos al sistema informático. Las *bombas zip* grafican esta modalidad, pues el usuario descarga un archivo comprimido que inundará el ordenador con millones de *bytes*. Por ejemplo, hay algunos archivos maliciosos que pasan de 42 kB a 5.5 GB. No obstante, considero que lo que

599 Meter o hacer entrar algo en otra cosa.

600 Espinoza Calderón, *Delitos informáticos y nuevas modalidades delictivas*, cit., p. 77.

601 Arévalo Minchola/Vega Aguilar, *Ciberdelitos. Análisis en el sistema penal*, cit., p. 272.

602 Vargas Carpio, Mónica Rocío. "Atentado a la integridad de datos informáticos (Artículo 3 de la Ley de Delitos Informáticos)". En: Espinoza Calderón, Víctor Raúl (coord.). *Cibercriminalidad y delitos informáticos*. Lima: Instituto Pacífico, 2023, p. 387.

603 Pérez López, *Delitos regulados en leyes penales especiales*, cit., p. 117.

se afecta realmente es el sistema informático. Por eso, hace algunos años indiqué que el verbo *introducir* no debería integrar el delito de atentado contra la integridad de los datos informáticos, sino contra los sistemas.

El artículo 5 del Convenio sobre la Ciberdelincuencia sí recoge la figura de *introducir datos informáticos*, pero relacionada a la obstaculización del sistema informático. De ahí que *introducir datos informáticos* como una figura de atentado contra los datos resulte algo confuso de interpretar o, incluso, posible de aplicar.

6.7.2.3. Borrar[604], *deletion*[605]

Colombia, Paraguay, Costa Rica, Panamá, República Dominicana y España incorporan este verbo rector en sus legislaciones. En Argentina, se utiliza el verbo *destruir* en vez de *borrar*[606].

Cierto sector de la doctrina identifica esta conducta como *vandalismo electrónico*, originalmente asociado al *ciberpunking*[607], toda vez que los atacantes apuntan a la destrucción de la información o de los datos informáticos del usuario.

Doctrina colombiana autorizada considera que "se trata de aquellos comportamientos informáticos que buscan hacer ilegibles o irrecuperables los

604 Desvanecer, quitar, hacer que desaparezca algo.

605 The act of removing something that has been written or printed, or that has been stored on a computer; something that has been removed.

606 "La voz 'destruir' se refiere a la eliminación definitiva, sin capacidad de recuperación. Debido a las características de los sistemas informáticos, puede darse el caso de que se haya borrado un archivo -es decir que éste desaparezca para el usuario del dispositivo-, pero que permanezca en el disco, y solo se eliminará cuando se sobrescriba con otro archivo o mediante un proceso de wipeado. En estos casos -en que se haya utilizado un borrado convencional y solo se quite el archivo del índice-, mediante técnicas de recuperación puede restaurarse. Otra opción es que efectivamente se haya efectuado un borrado seguro de la información y que sea irrecuperable. De esto se colige la importancia de conocer las técnicas utilizadas por los autores de la acción dañosa y su impacto en el sistema informático. De ello dependerá -de un análisis caso a caso- la subsunción de la conducta desplegada en la previsión del Código y, a su vez, en los medios comisivos previstos en la norma" (Kiefer, "Daño informático", cit., p. 329).

607 Aboso, *Derecho penal cibernético*, cit., p. 360. En la misma línea, Lledó Benito, *Formas específicas de criminalidad*, cit., p. 135.

datos, sin necesidad de eliminarlos, en el medio de almacenamiento o del *software* aplicativo u operativo que permite que funcionen los sistemas informáticos"[608], sin embargo, acota que este verbo rector debe ser analizado no desde el sentido común, sino técnico. De este modo, "[d]ebe tratarse de una acción técnica que reescriba los datos informáticos. En principio, el borrado se debe interpretar en sentido técnico y, aunque no es claro, consideramos que la posibilidad de recuperar el fichero 'borrado' impide aplicar el tipo penal como se ha citado, pues, en realidad, el falso borrado es una obstaculización al acceso o funcionamiento normal de los datos informáticos"[609].

De otro lado, Vega Aguilar y Arévalo Minchola sostienen que "esta modalidad tendría como objetivo desaparecer un determinado dato o parte de un dato informático para provocar que no cumpla la función y/o labor que originalmente debía lograr"[610]. En línea similar, Pérez López considera que significa "desvanecer, quitar, hacer que desaparezca algo"[611], al igual que Vargas Carpio, para quien es la "acción de eliminar datos sistemáticos de un sistema o base de datos"[612].

Considero que borrar datos informáticos es el equivalente a destruir un objeto físico, tangible. Así, de todas las conductas, es la única que elimina técnicamente la existencia del dato informático. Por ejemplo, luego de infectar un dispositivo electrónico, algunos virus, como el *ranscam*, borran o eliminan importantes archivos (datos) del sistema que, luego, no pueden ser recuperados. En esta misma línea, el Informe Explicativo emplea la siguiente comparación: "El borrar datos es el equivalente de la destrucción de un objeto corpóreo. Los destruye y los hace irreconocibles".

Hay quienes consideran que, aunque los datos o documentos destruidos puedan ser recuperados, el ilícito se configura porque "la falta de disposición

608 Posada Maya, *Los cibercrímenes*, cit., p. 354.

609 Ibidem.

610 Arévalo Minchola/Vega Aguilar, *Ciberdelitos. Análisis en el sistema penal*, cit., p. 274.

611 Pérez López, *Delitos regulados en leyes penales especiales*, cit., p. 117.

612 Vargas Carpio, "Atentado a la integridad de datos informáticos (Artículo 3 de la Ley de Delitos Informáticos)", cit., p. 387.

sobre esos documentos es razón suficiente para afirmar su tipicidad"[613]. Coincido que esta acción configura un delito, pero no la modalidad estudiada, sino la de *suprimir*, ya que borrar equivale a su destrucción irrecuperable; mientras que al suprimirlos se pone fin a su disposición -que puede ser temporal-.

Espinoza Calderón precisa que la norma no especifica si la eliminación ha de ser remota o presencial[614]. Considero que ambas posibilidades son perseguibles penalmente, pues nuestra legislación no exige que el borrado sea a distancia. En esta línea, la profesora Alicia Gil Gil explica que el caso típico de borrado, mediante acceso directo al sistema, es el del empleado insatisfecho que borra sus archivos al ser despedido de la empresa. En cambio, los ataques remotos más conocidos son los realizados mediante *malwares*[615].

En conclusión, borrar datos informáticos equivale a destruirlos permanentemente. Siendo esto así, es una de las conductas más graves que un atacante podría cometer en contra de la seguridad informática.

[Caso 71] Los WD My Book son un servidor NAS con un diseño vertical que le permite al usuario almacenar y acceder a sus archivos de forma remota. En el 2021, los investigadores de Western Digital detectaron vulnerabilidades que permitieron que ciberdelincuentes accedan de forma remota a "My Book Live NAS" y puedan restaurar los dispositivos (restablecimiento de fábrica). De este modo, los usuarios podían acceder a las carpetas iniciales, pero sus archivos desparecieron, fueron eliminados.

Para realizar estos restablecimientos, los delincuentes utilizaron ataques de Zero-day. Así, si los atacantes logran determinar los parámetros correctos de acceso al punto final, podían ejecutar desencadenantes masivos y, de este modo, reestablecer todos los dispositivos objetivo-afectados[616].

613 Aboso, *Derecho penal cibernético*, cit., p. 359.

614 Espinoza Calderón, *Delitos informáticos y nuevas modalidades delictivas*, cit., p. 77.

615 Gil Gil, Alicia. "Daños informáticos". En: Sanz Delgado, Enrique y Daniel Fernández Bermejo (coords.). *Tratado de delincuencia cibernética*. Navarra: Thomson Reuters / Aranzadi, 2021, p. 478.

616 Centro Nacional de Seguridad Digital. *Alerta integrada de seguridad digital N.º 161-2021*. Lima: 1 de julio de 2021, p. 4. https://www.gob.pe/institucion/pcm/

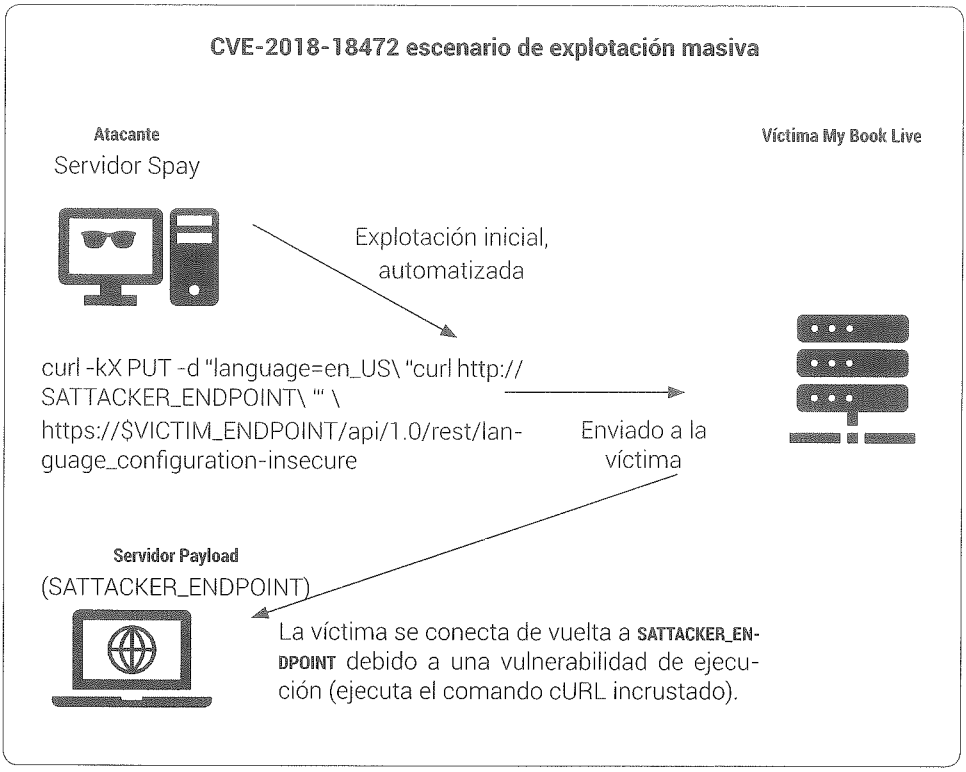


Diagrama 12. Solicitud de ejemplo, vista desde el servidor controlado por el atacante desde la víctima My Book Live. Adaptación, a partir de CENSYS[617].

[Caso 72] Un *wiper* es un *malware* que elimina datos de los sistemas informáticos. El ciberdelincuente o quienes están detrás no buscan dinero a cambio del rescate de la información, como en el caso de los *ransomware*, sino destruir la data almacenada en objetivos específicos.

En el 2012, el *wiper* Shamoon (W32.Disttrack) fue utilizado para atacar centros de abastecimiento energético de Arabia Saudita. Este *malware* infectó 35 mil computadoras de una compañía petrolífera de Oriente Medio y

informes-publicaciones/2002739-alerta-integrada-de-seguridad-digital-n-161-2021-pecert

617 "CVE-2018-18472: Explotación masiva de Western Digital My Book Live", publicada el 29 de junio de 2021 yt actualizada al 2 de julio. Disponible en: https://censys.com/es/cve-2018-18472-western-digital-my-book-live-mass-exploitation/

puso en peligro el suministro del 10 % mundial de petróleo[618]. Este ataque coordinado (1) infectaba máquinas en la red interna, (2) utilizaba alguna de ellas como proxy y (3) luego de cuatro horas, recolectaba nombres y destruía ficheros (datos informáticos). Según especialistas en ciberseguridad, "[e]s difícil predecir qué datos se perderán de forma irreversible y cuales seguirán intactos después de la 'limpieza' -depende del tamaño de los archivos guardados en el ordenador infectado y de cómo estén distribuidos en el disco duro"[619].

Se apuntó a Irán como el origen del ataque, pues, el 17 de noviembre, Shamoon comenzó a *limpiar* todos los archivos infectados, pero dejó como recordatorio la imagen de Alan Kurdi, un niño refugiado sirio de tres años que fue asesinado en las playas de Turquía[620].

6.7.2.4. Deteriorar[621], *deterioration*[622]

A nivel comparado, la legislación de Colombia y España recogen esta conducta.

Para la doctrina colombiana, "se trata de un verbo típico derivado del daño. Sin embargo, el deterioro hace referencia a la disminución de la funcionalidad de los datos almacenados o tratados por los sistemas de tratamiento de información, sus partes o sus componentes lógicos, teniendo en cuenta su estado previo. Este verbo implica un menor desvalor del resultado que la destrucción o borrado de la información"[623].

---

618 Hispasec. *Shamoon: un malware que destruye los datos y el sistema*, publicado el 19 de agosto de 2012. https://unaaldia.hispasec.com/2012/08/shamoon-un-malware-que-destruye-los-datos-y-el-sistema.html

619 Kaspersky. *Shamoon el limpiador: más detalles (Parte II)*, publicado el 13 de setiembre de 2012. https://securelist.lat/shamoon-el-limpiador-ms-detalles-parte-ii/65799/

620 Pagliery, José. *Hackers destruyen computadoras saudíes con el arma digital más poderosa del mundo*, publicado por la CNN el 2 de diciembre de 2016. https://cnnespanol.cnn.com/2016/12/02/hackers-destruyen-computadores-saudies-con-el-arma-digital-mas-peligrosa-del-mundo

621 Empeorar, degenerar.

622 The fact or process of becoming worse.

623 Posada Maya, *Los cibercrímenes*, cit., pp. 354 y s.

Cierto sector de la doctrina nacional la define como "causar daños a los datos informáticos originando su pérdida total o parcial"[624] o la "acción de causar daño o desgaste a los datos sistemáticos, ya sea de forma natural o intencional"[625]. Considero que esta definición no es adecuada, pues utiliza una conjugación del verbo dañar en su desarrollo, lo que generará problemas de interpretación con la primera forma aquí estudiada, esto es, dañar datos informáticos.

Para otro sector académico, "esta modalidad típica consiste en hacer que una cosa pase a tener peor estado o que tenga menos valor que antes [...] se podría indicar que se presentará esta modalidad cuando se ocasione una cierta lesión al dato informático, pero que no lo elimine ni lo desaparezca, empero sí lo haga menos valorizado"[626]. En similar posición se sostiene que es "empeorar, degenerar una base de datos"[627].

Deteriorar datos informáticos significa empeorar o degenerar su calidad, sin alterar su estructura. Así, si un virus infecta algunos archivos y los vuelve pesados, dificulta su lectura, pues cada vez que los abro demora no solo para acceder a estos, sino al cambiar de página en página, entonces podremos afirmar que los datos informáticos han sido deteriorados.

Como habrá notado el lector, líneas arriba indiqué que el parágrafo 61 del Informe Explicativo define los verbos *dañar* y *deteriorar* en el mismo párrafo -lo que dificulta una adecuada diferenciación e interpretación.

6.7.2.5. Alterar[628], *altering*[629]

Colombia, Argentina, Chile, Panamá y España recogen esta figura.

En Argentina, se sostiene que, en este supuesto, "un archivo digital no presentará la información que contenía originalmente, pues ha sido modificado,

624 Espinoza Calderón, *Delitos informáticos y nuevas modalidades delictivas*, cit., p. 77.

625 Vargas Carpio, "Atentado a la integridad de datos informáticos (Artículo 3 de la Ley de Delitos Informáticos)", cit., p. 387.

626 Arévalo Minchola/Vega Aguilar, *Ciberdelitos. Análisis en el sistema penal*, cit., p. 274.

627 Pérez López, *Delitos regulados en leyes penales especiales*, cit., p. 117.

628 Cambiar la esencia o forma de algo

629 To become different; to make somebody/something different.

pero no destruido ni inutilizado. En relación con los programas informáticos, supone un cambio en su funcionamiento"[630].

En Colombia, "significa que se cambia o modifica en todo o en parte la esencia, la forma o el contenido de los datos existentes, de los sistemas de tratamiento de información, sus partes o los componentes lógicos. La alteración se puede lograr mediante adición, supresión o creación de datos o rutinas, sin que para esto se vea afectada necesariamente la disponibilidad o capacidad de tratamiento del sistema informático"[631].

En España se afirma que "la alteración se integra por comportamientos de inserción de datos, modificación o supresión parcial que origina una perturbación funcional definitiva"[632].

La doctrina nacional define este término como "manipular los datos a conveniencia de la persona que realiza el delito, modificando la información original"[633] o "la acción de modificar datos sistemáticos de una manera que cambia su significado o impacto"[634]. En la misma línea, "esta modalidad tiene lugar cuando el sujeto modifica, cambia o fragua información del dato o aspectos del dato informático. Para poder hablar de alteración debemos tener presente que debe existir una manipulación y/o modificación del dato informático y sus componentes"[635]. Por *alterar* "se ha de entender la modificación del estado en que se encontraba el bien, la manipulación del soporte lógico, esto es, los datos y/o programas contenidos en la computadora. No implica un enriquecimiento directo para el sujeto activo, aun cuando pueda derivarse de uno indirecto"[636].

El Informe Explicativo recoge la siguiente definición: "El término alteración se refiere a la modificación de los datos existentes. Por consiguiente, la introducción de códigos maliciosos, tales como virus y caballos de Troya, está

630 Kiefer, "Daño informático", cit., p. 328.

631 Posada Maya, *Los cibercrímenes*, cit., p. 355.

632 Barrio Andrés, *Delitos 2.0. Aspectos penales, procesales y de seguridad de los ciberdelitos*, cit., p. 110.

633 Espinoza Calderón, *Delitos informáticos y nuevas modalidades delictivas*, cit., p. 77.

634 Vargas Carpio, "Atentado a la integridad de datos informáticos (Artículo 3 de la Ley de Delitos Informáticos)", cit., p. 387.

635 Arévalo Minchola/Vega Aguilar, *Ciberdelitos. Análisis en el sistema penal*, cit., p. 274.

636 Pérez López, *Delitos regulados en leyes penales especiales*, cit., p. 117.

incluido en este párrafo, tal como también lo está la modificación resultante de los datos".

Sostengo que alterar datos informáticos significa cambiar o variar la forma que originalmente se les asignó. El usuario podrá acceder a los datos informáticos, pero no tendrán la misma estructura o contenido. Por ejemplo, algunos troyanos infectan archivos y reemplazan sus nombres por símbolos o caracteres que dificulta identificarlos. En este caso, considero, los datos informáticos han sido alterados.

[**Caso 73**] Si definimos una página web como un documento estructurado que contiene datos informáticos, podemos afirmar que un ataque de desfiguración, llamado *defacement*, altera su estructura y, en consecuencia, es un atentado contra la integridad de los datos informáticos (y no de un sistema informático). Dicho esto, en febrero del 2021, se detectó un ataque de *defacement* a la página web de la Municipalidad Distrital de Ate, Lima. Cuando un visitante ingresaba a la web en referencia, veía la siguiente imagen, que incluye el alias del atacante «K4TSUY4-GHO5T»:

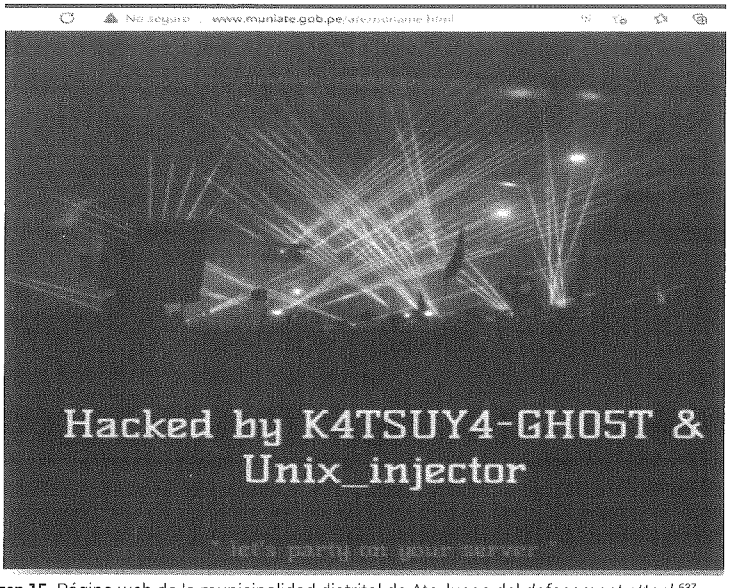


Imagen 15. Página web de la municipalidad distrital de Ate, luego del *defacement attack*[637].

637 Alerta Integrada de Seguridad Digital N.º 036.

[**Caso 74**] Un ataque similar se suscitó el 11 de marzo del 2025, pero se dirigió a la página web de la municipalidad de Pucusana. En este caso, Deface Peru se adjudicó el ataque. Es importante señalar que si los ciberdelincuentes, además, eliminan archivos esenciales para el funcionamiento o explotan vulnerabilidades para obtener acceso de administrador al sistema, entonces el delito no será de atentado contra los datos, sino contra los sistemas informáticos.

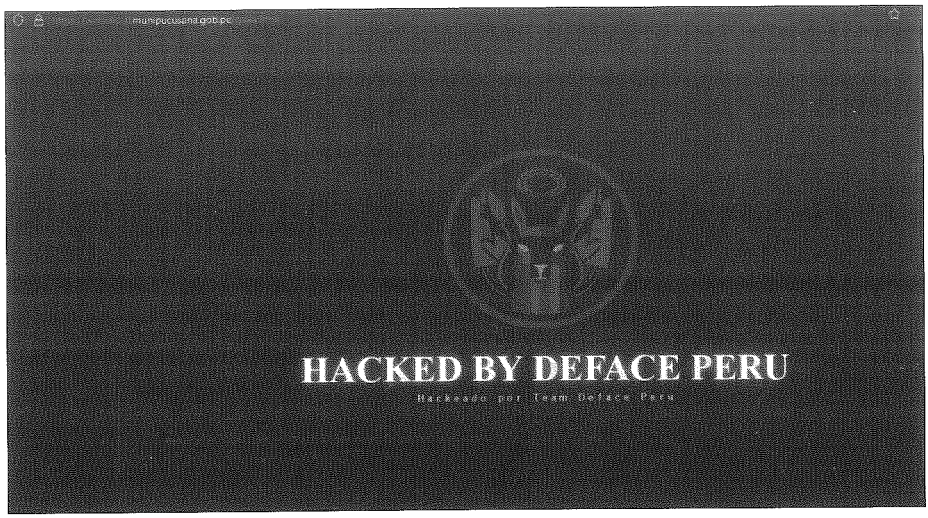


Imagen 16. Página web de la municipalidad de Pucusana, luego del *defacement attack*[638].

6.7.2.6. Suprimir[639], *suppressing*[640]

A nivel comparado, Colombia, Paraguay, Costa Rica, Chile, Panamá y España adoptan esta modalidad.

En la doctrina colombiana, se precisa que "esta conducta comporta hacer desaparecer datos informáticos o los comportamientos lógicos del sistema, afectando su disponibilidad para los usuarios o administradores legítimos. Por

638 La imagen fue obtenida de @Alph4_Sec.

639 Hacer cesar, hacer desaparecer.

640 To prevent something from being published or made known.

el contrario, la destrucción está dirigida a sancionar la pérdida grande y casi irreparable de las partes del sistema de tratamiento de datos o de la información"[641].

Víctor Espinoza lo define como "desaparecer un dato informático de su ubicación original"[642]. Este concepto es compartido por Vega Aguilar y Arévalo Minchola: "Esta modalidad típica implica la desaparición completa de un determinado dato informático. Este verbo viene a consolidar el conjunto de modalidades típicas esbozadas y retrata el hecho de eliminar completamente el dato informático"[643]. Para Pérez López significa "hacer cesar, hacer desaparecer una base de datos"[644], mientras que para Vargas Carpio es la "acción de eliminar intencionalmente datos sistemáticos de un conjunto de información, a menudo con la intención de ocultar información"[645].

Este verbo rector ha sido definido en el Informe Explicativo en los siguientes términos: "Por supresión de datos informáticos se entiende cualquier acción que impida o ponga fin a la disponibilidad de los datos para la persona que tiene acceso al ordenador o al soporte de datos en que fueron almacenados".

Considero que suprimir datos informáticos es impedir o poner fin a su disponibilidad para el usuario que tiene acceso al ordenador o al soporte de datos en que fueron depositados, ya que han sido ocultados o desindexados por el atacante.

[Caso 75] A modo ilustrativo he de indicar que existen *virus de acceso directo* que *desaparecen* u ocultan los archivos de un USB al conectarlos a un ordenador. Así, los archivos siguen allí, no han sido eliminados, pero el usuario no puede observarlos o disponer de ellos.

> Los virus de acceso directo son programas maliciosos que pueden infectar tu ordenador y hacer que se creen accesos directos en tu es-

641 Posada Maya, *Los cibercrímenes*, cit., p. 355.

642 Espinoza Calderón, *Delitos informáticos y nuevas modalidades delictivas*, cit., p. 77.

643 Arévalo Minchola/Vega Aguilar, *Ciberdelitos. Análisis en el sistema penal*, cit., pp. 274 y s.

644 Pérez López, *Delitos regulados en leyes penales especiales*, cit., p. 117.

645 Vargas Carpio, "Atentado a la integridad de datos informáticos (Artículo 3 de la Ley de Delitos Informáticos)", cit., p. 387.

> critorio o en la lista de archivos del Explorador de Windows. Estos virus pueden propagarse a través de adjuntos de correo electrónico, descargas de sitios web infectados e incluso unidades USB. Aunque inicialmente no parezcan dañinos, los virus de acceso directo pueden provocar problemas graves como la pérdida o corrupción de datos.
>
> [...]
>
> Los virus de los accesos directos pueden causar problemas en tu ordenador de varias maneras. En primer lugar, pueden crear nuevos accesos directos en tu escritorio o en tu lista de archivos del Explorador de Windows. Estos accesos directos pueden apuntar a programas o archivos que no existen, lo que dificulta encontrar los archivos que buscas. Además, los virus de los accesos directos pueden cambiar los iconos asociados a estos accesos directos, lo que hace aún más difícil averiguar qué se supone que deben hacer[646].

Lamentablemente, durante la pandemia del COVID-19, este tipo de *malware* se distribuyó a través de correos electrónicos o archivos adjuntos que contenían supuesta información sobre la enfermedad y su tratamiento[647].

[Caso 76] Carlos Christian Sueiro plantea un caso que permite diferenciar *borrar* y *suprimir* datos informáticos:

> Martín es un joven ingeniero en sistemas que le gusta experimentar, a veces sin conocer las consecuencias legales de sus actos.
>
> Un buen día, al solo fin de irritar a su compañero de oficina Leopoldo, accede vía remota a su computadora, y envía a la papelera de reciclaje un balance en el que estuvo trabajando durante una semana.
>
> Leopoldo, desesperado, no entiende qué ocurrió, y entra en pánico al saber que debe entregarlo al día siguiente.
>
> Al otro día, Leopoldo sin dormir tiene casi listo un borrador nuevo del balance.

646 Easeus. *Todo lo que necesitas saber sobre el virus de acceso directo*, publicado el 14 de marzo de 2015. https://es.easeus.com/recuperar-datos/virus-de-acceso-directo.html

647 Kaspersky. *El coronavirus ha llegado a la web: Kaspersky*, publicado el 30 de enero de 2020. https://latam.kaspersky.com/about/press-releases/el-coronavirus-ha-llegado-a-la-web-kaspersky

> Sin embargo, Clarisa, otra compañera de Leopoldo, le dice que le permita chequear su computadora, y constata que el balance está en la papelera de reciclaje, la cual no se ha vaciado.
>
> Es así que restaura el documento y recupera el balance[648].

6.7.2.7. Hacer inaccesible

A nivel comparado, España recoge esta modalidad. En otras latitudes, se emplea la expresión *inutilizar* y puede ocurrir cuando el autor instala un programa que impide al titular acceder de manera libre a los datos informáticos, mediante la instalación de un acceso restringido[649].

A nivel local, algunos autores definen esta modalidad como "ocultar los datos informáticos"[650], otros sostienen que "esta modalidad típica viene a ser una introducción inédita del legislador peruano y tiene como finalidad el cierre de espacios de impunidad que pudieran existir. Hacer inaccesible implica lograr que el dato informático sea no utilizable para su propietario, lo cual implicaría previamente alguna de las modalidades como alterar, introducir o suprimir el dato informático"[651]. Otros tantos lo definen como la "acción de impedir que los datos sistemáticos sean accesibles por parte de los usuarios autorizados o legitimados"[652].

---

648 Sueiro, Carlos Christian. *Casos de criminalidad informática y prueba digital. Casos de inteligencia artificial (IA). Sistematización de jurisprudencia*. Buenos Aires: Ad-Hoc, 2022, pp. 80 y s.

649 Aboso, *Derecho penal cibernético*, cit., p. 361. "El verbo inutilizar hace referencia a la imposibilidad de practicar el uso habitual para cuyo fin existía el objeto. No implica destrucción o eliminación total del archivo, programa o sistema, sino que éstos no funcionen: puede eliminarse un byte de un archivo ejecutable, y éste no servirá para su finalidad. Asimismo, puede modificarse la extensión de un archivo, y el ordenador no lo reconocerá" (Kiefer, "Daño informático", cit., pp. 329 y s).

650 Espinoza Calderón, *Delitos informáticos y nuevas modalidades delictivas*, cit., p. 77.

651 Arévalo Minchola/Vega Aguilar, *Ciberdelitos. Análisis en el sistema penal*, cit., p. 275.

652 Vargas Carpio, "Atentado a la integridad de datos informáticos (Artículo 3 de la Ley de Delitos Informáticos)", cit., p. 388.

Sostengo que hacer inaccesibles datos informáticos es colocar un obstáculo que impide su acceso. Así, por ejemplo, el virus *HappyDayzz* encripta los archivos de un ordenador, es decir, siguen allí, el usuario los puede ver, pero no puede acceder a ellos porque existe un obstáculo: han sido cifrados por el ciberdelincuente. A diferencia de la modalidad *suprimir*, en este caso, no han desaparecido, pues el usuario puede navegar por el ordenador, abrir las carpetas y ver que los archivos se encuentran en la misma ubicación o que su peso no ha variado; sin embargo, existe una limitación que le impide utilizarlos.

[Caso 77] A inicios del 2021, el Equipo de Respuesta ante Incidentes de Seguridad Digital Nacional advirtió sobre la propagación de un tipo de *ransomware* denominado Vovalex. Este *software* malicioso se distribuye a través de supuestas aplicaciones de Windows como CCleaner, que ofrecen optimizar el sistema operativo.

Una vez descargado e instalado este utilitario, comienza a cifrar todos los archivos del sistema, agregando la extensión ".vovalex". Luego de algunos minutos, cuando finaliza el encriptado de todos los archivos, aparece una nota de rescate -a través de un archivo de texto llamado readme.vovalex.txt- que contiene las instrucciones para el pago y liberación de los datos secuestrados[653].

653 Centro Nacional de Seguridad Digital. *Alerta integrada de seguridad digital N.º 24-2021*. Lima: 2 de febrero de 2021, p. 3. https://www.gob.pe/institucion/pcm/informes-publicaciones/1639099-alerta-integrada-de-seguridad-digital-n-024-2021-pecert

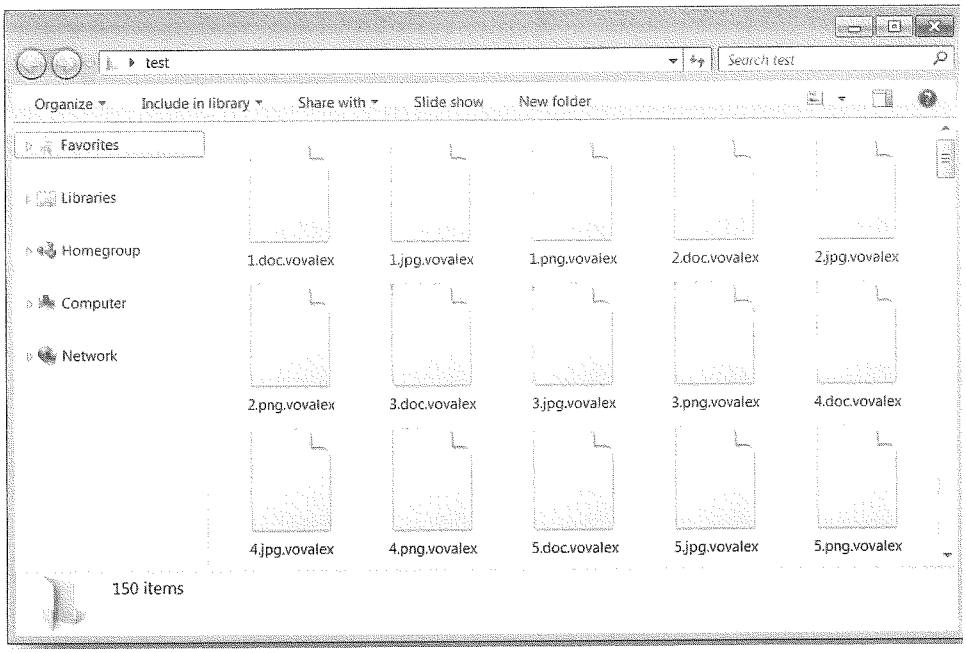


Imagen 17. Vista de una carpeta cuyos archivos fueron encriptados por el *ransomware Vovalex*[654].

Si ya de por sí comprender los términos técnicos y sus diversas modalidades representa una tarea compleja, la interpretación jurídica no debería añadirle mayor dificultad. Por ello, a modo de resumen, a continuación, se presentan de forma sintetizada las definiciones propuestas en este apartado:

Verbos	Definición propuesta
Introducir	Ingresar datos informáticos.
Alterar	Modificar o variar el contenido, la estructura o el formato de los datos informáticos.
Deteriorar	Empeorar o degenerar la calidad de los datos informáticos, sin afectar su estructura.
Hacer inaccesible	Obstaculizar el acceso al dato informático, ya que si bien es visible no puede ser abierto ni manipulado.
Suprimir	Impedir la disponibilidad del dato informático, pues ha sido ocultado o desindexado.
Borrar	Eliminar permanentemente el dato informático, impidiendo su recuperación.
Dañar	Causar detrimento, perjuicio o menoscabo de los datos informáticos. Es una conducta residual.

Cuadro 22. Resumen de definiciones propuestas de los verbos que integran delito de atentado a la integridad de datos informáticos. Elaboración propia.

654 Bleeping Computer. *Vovalex is likely the first ransomware written in D*, publicado el 29 de enero de 2021. https://www.bleepingcomputer.com/news/security/vovalex-is-likely-the-first-ransomware-written-in-d/

6.7.3. Objeto del delito: datos informáticos

A nivel local, se ha sostenido que las distintas modalidades delictivas recaen sobre la información contenida en los sistemas informáticos, con el propósito de perturbarla, destruirla o modificarla. Discrepo de dicha postura, en la medida en que el objeto del delito no es la *información* en sí misma, sino los *datos informáticos*, conforme a las definiciones desarrolladas en los capítulos precedentes.

En este sentido, la doctrina autorizada precisa que "el objeto material del delito sería el soporte lógico y los datos contenidos en el sistema, pues resulta claro que los daños en el *hardware* se regulan por el régimen tradicional, pues, por la concepción de la propiedad y del tipo de bienes sobre los cuales la misma puede recaer, los datos y en general la información almacenada o procesada por las altas tecnologías presentarían serios inconvenientes para servir como objeto material del delito de daños"[655].

A continuación, se presentan dos casos relevantes: el primero involucra el acceso no autorizado a las cuentas de docentes universitarios para modificar las calificaciones de un estudiante; el segundo, un ataque en el que se alteraron las calificaciones de más de 18 mil alumnos en una sola acción.

[Caso 78] Entre el 2 de abril de 2017 y el 31 de enero de 2018, Severino y Carlos Jesús llevaron a cabo múltiples accesos fraudulentos a las cuentas de usuario de varios docentes del Doble Grado en Administración de Empresas e Ingeniería en Tecnologías y Servicios de la Telecomunicación. A través de estos accesos, procedieron a modificar las calificaciones de Carlos Jesús en diversas asignaturas, tales como Métodos Estadísticos y Economía, Microeconomía II, Fundamentos de Sistemas Digitales, Arquitecturas Telemáticas II, Circuitos Electrónicos y Dispositivos Electrónicos. Para obtener las credenciales necesarias y alterar dichas notas, utilizaron un *keylogger*, cuya presencia fue detectada el 2 de febrero de 2018[656].

655 Pérez López, *Delitos regulados en leyes penales especiales*, cit., p. 117 y 120.

656 SJP 36/2020. Sentencia N.º 267/2020 del 24 de setiembre 2020, emitida por el Juzgado de Valencia, Sección N.º 12. Ponente: Margarita Sierra Serrano.

En España, según la imputación y marco normativo, fueron condenados por falsedad de documento oficial en concurso medial con el delito de descubrimiento y revelación de secretos. Si analizamos el caso bajo la LDI, la modificación de las notas constituye un supuesto de alteración de datos informáticos.

[Caso 79] En Colombia, la universidad de Tolima reportó un caso mucho más grave. Durante la temporada de vacaciones del 2018, un ciberdelincuente accedió a sus sistemas informáticos y modificó las notas de todos los alumnos, el histórico de calificaciones, promedios semestrales y hasta los datos de los estudiantes egresados.

Felizmente, según sus autoridades administrativas, la universidad contaba con copias de seguridad que les permitió recuperar rápidamente la información. Un estudiante entrevistado por el diario *El Tiempo* manifestó: "Cuando vi mis calificaciones en cinco, me dio cierta alegría, pero al instante reaccioné y dije: 'aquí pasó algo raro pues mis notas no han sido las mejores'"[657].

6.8. TIPICIDAD SUBJETIVA

Esta conducta solo admite figuras dolosas, descartándose las actuaciones culposas. Toda vez que el legislador incluyó la acepción *deliberadamente*, podemos recomendar interpretarla como una exclusión a la tercera manifestación del dolo, esto es, el dolo eventual.

Algunos autores peruanos sostienen que la inclusión del elemento deliberado "ha venido a complementar el aspecto subjetivo, dotando con claridad la exigencia de presentación de dolo directo para la comisión del referido delito"[658]. Considero que, de un lado, no era necesaria esta inclusión, pues el Convenio de Budapest utiliza este elemento para remarcar que se sancionan dolosas -no

657 El Tiempo. *Hacker mejoró notas de los estudiantes de la Universidad de Tolima*, publicado el 1 de febrero de 2018. https://www.eltiempo.com/colombia/otras-ciudades/hacker-mejoro-las-notas-de-todos-estudiantes-de-la-universidad-del-tolima-177850

658 Arévalo Minchola/Vega Aguilar, *Ciberdelitos. Análisis en el sistema penal*, cit., p. 282.

culposas-[659], de otro, porque ningún país de la región latinoamericana que se ha adherido al citado Convenio ha incluido esta fórmula y, finalmente, porque dificulta la labor de investigación y prueba, excluyendo casos en los que el ciberdelincuente actúe bajo una modalidad de dolo eventual.

6.9. LAS SITUACIONES DE JUSTIFICACIÓN EN EL DELITO DE ATENTADO CONTRA LOS DATOS INFORMÁTICOS

El legislador ha reiterado que esta conducta debe ser ejercida *ilegítimamente*, es decir, si existe una causa de justificación, entonces no será antijurídica. Oré Sosa, de manera acertada, precisa que la autorización excluye la ilicitud de la conducta y, consecuentemente, la imputación del comportamiento[660]. De este modo, si el soporte informático de mi oficina elimina archivos maliciosos (*malware*) de la computadora que he entregado para revisión y mantenimiento, la conducta no será antijurídica.

El parágrafo 62 del Informe Explicativo describe aquellas conductas que integran la ejecución de pruebas del sistema autorizadas por los usuarios:

> Las actividades comunes inherentes al diseño de las redes o las prácticas comerciales o de operación comunes como, por ej., la verificación o la protección de la seguridad de un sistema informático autorizadas por el dueño o el operador, o la reconfiguración del sistema operativo de un ordenador que tenga lugar cuando el operador de un sistema adquiere un nuevo *software* (por ej., el *software* que permite el acceso a Internet que desactiva programas similares instalados previamente), son efectuadas de manera legítima y, en consecuencia, no constituyen un delito conforme a este artículo. La modificación de los datos relativos al tráfico con el fin de facilitar comunicaciones anónimas (por ejemplo, las actividades de los sistemas de redireccionamiento de mensajes de correo electrónico anónimos), o la modificación de datos con el fin de garantizar la seguridad de las comunicaciones (por ej., el cifrado) deberían en principio ser consideradas una forma de protección

659 En esta línea, Meneses Gonzáles/Meneses Ochoa, *La cibercriminalidad: Consideración criminológica, político-criminal, dogmática, procesal y cooperación internacional*, cit., p. 313.

660 Oré Sosa, *Delictum. Apuntes de derecho penal*, cit., p. 195.

legítima de la vida privada y, por lo tanto, ser consideradas actividades legítimas.

Como se ha señalado con anterioridad, dada la construcción propia del ordenamiento peruano, no es necesario precisar que la actuación debe ser *ilegítima*. De hecho, a nivel comparado, no se ha encontrado otra legislación que recoja tal elemento.

[Caso 80] En el 2015, Joaquín Sorianello advirtió que el *software* desarrollado por la empresa MSA tenía un fallo de seguridad, ya que se habían filtrado los certificados SSL que aseguraban las comunicaciones de las computadoras de votación con la Cámara Electoral de Argentina. Esta brecha abría la posibilidad de generar resultados falsos. Luego de comprobar el referido problema de seguridad, Sorianello se comunicó con la empresa y le informó sus hallazgos. Poco tiempo después, una jueza ordenó el allanamiento de su vivienda y el inicio de un proceso judicial en su contra.

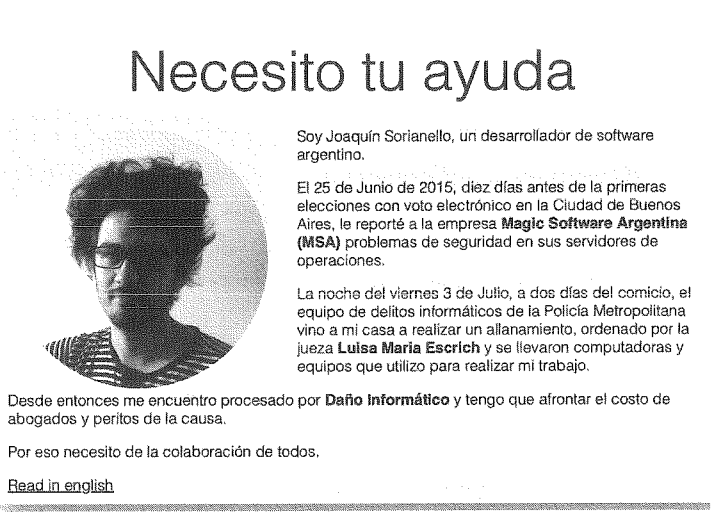


Imagen 18. El procesamiento de Joaquín Sorianello puso los reflectores sobre la vulnerabilidad de los sistemas de voto electrónico del gobierno de la Ciudad de Buenos Aires[661].

661 El Cordillerano. *Todos los sistemas de voto electrónico tienen problemas*, publicado el 5 de agosto de 2016. https://www.elcordillerano.com.ar/noticias/2016/08/05/57865-todos-los-sistemas-de-voto-electronico-tienen-problemas
La campaña de donación se alojó en Github. El anuncio aún se encuentra disponible en: https://joac.github.io/donations/

La investigación concluyó que los sistemas informáticos no sufrieron daños y que, en efecto, Sorianello colocó una bandera en los sistemas como señal de acceso, además de notificar a la compañía sobre el hallazgo de la brecha de seguridad[662]. El caso fue archivado:

> [...] Consecuentemente, se ordenó el allanamiento de dicha finca y se comprobó que Joaquín Sorianello residía allí junto a su novia. Además, se secuestraron todos los elementos para el caso, conforme surge de las actuaciones labradas en consecuencia y lucen a fs. 143/160. Luego de ello se dispuso la realización de un estudio pericial sobre los efectos incautados a fin de determinar si desde dichos dispositivos se ingresó al servidor caba.operaciones.com.ar y en caso afirmativo se especifique la maniobra desarrollada, como así también si poseían algún archivo con información sensible que pertenezca al "Grupo MSA" -ver fs. 172, 192 y 193-. Asimismo, la defensa del nombrado presentó otros puntos de pericia que lucen a fs. 194 y 260/277, y el 4 de setiembre de 2015 se inició el informe técnico habiendo finalizado el 14 de julio de este año. Ahora bien, del análisis del informe realizado por el Oficial Carnero de la Policía Metropolitana, se desprende que en los dispositivos secuestrados en el domicilio de Sorianello, se detectaron noventa y un (91) accesos al servidor de caba.operaciones.com.ar con la creación de un evento PWONED, pero no se encontró ningún archivo de interés o dato sensible de la empresa denunciante -ver fs. 347-. Explicó el oficial que el concepto PWONED en términos de informática significa que el pequeño (una persona) encuentra una vulnerabilidad a un grande (una empresa), donde se utiliza colocar una bandera (como símbolo) para informar que el sistema desarrollado por la empresa es vulnerable. Esta bandera no genera ningún daño o alteración al normal funcionamiento del sistema informático en cuestión (sic). Cabe resaltar que dicha explicación se condice con lo que surge de la con-

662 La Nación. *Sobreseyeron al programador que reveló fallas en el sistema de voto por Boleta Única Electrónica*, publicado el 2 de agosto de 2016. https://www.lanacion.com.ar/tecnologia/sobreseyeron-al-programador-que-revelo-fallas-en-el-sistema-de-boleta-unica-electronica-nid1924088/
En el mismo sentido: Página 12. *De ciberterrorista a ciudadano alerta*, publicado el 4 de agosto de 2016. https://www.pagina12.com.ar/diario/elpais/1-305974-2016-08-04.html

> versación mantenida entre Sorianello y [...] empleado de la empresa damnificada, aportado por la defensa a fs. 262/277, la cual también ha sido peritada -ver soporte óptico de fs. 351-. En definitiva, de los elementos incorporados al presente, se advierte que, si bien se acreditó que Joaquín Sorianello ingresó al sistema informático de la empresa Grupo MSA, no lo hizo de manera indebida ni causó daño alguno, sino que, por el contrario, lo hizo para dar aviso a la firma de que el sistema de seguridad era vago y podía ser vulnerado con facilidad. Es por los motivos expuestos, y considerando que la conducta desplegada por el mencionado no encuadra en figura penal alguna, conforme lo normado por el artículo 199, inc. a) del CPPCABA, RESUELVO: Archivar el caso [...][663].

En este caso, se advierte que existe un acceso ilegítimo o ilícito, pero no un ataque a la integridad de un sistema informático. Si utilizamos la legislación peruana, podríamos concluir que se configura el delito de atentado a la integridad de los datos informáticos, en la modalidad de *insertar datos informáticos*. Ciertamente, Joaquín no tenía autorización para ingresar al sistema y, mucho menos, para generar el evento "PWNOED", esto es, insertar o colocar una *bandera* que permitiese identificar la brecha de seguridad y, de este modo, la compañía pudiese arreglarlo -evitando de este modo, posibles ataques-.

Considero que tanto el acceso ilícito como el ataque a la integridad de los datos informáticos se configuran en el caso de Joaquín Sorianello: tenía la intención de ingresar, sin autorización, e insertar datos informáticos en un sistema ajeno. El artículo 12 LDI no es aplicable, pues su tenor señala expresamente:

> **Art. 12 LDI.-** Está exento de responsabilidad penal el que realiza las conductas descritas en los artículos 2, 3, 4 y 10 con el propósito de llevar a cabo pruebas autorizadas u otros procedimientos autorizados destinados a proteger sistemas informáticos.

663 La resolución se encuentra disponible en: https://pupilacdn.nyc3.cdn.digitaloceanspaces.com/diariojudicial.public/documentos/000/069/661/000069661.pdf

Como se ha dicho, Joaquín Sorianello no tenía autorización, es decir, no realizó pruebas o procedimientos autorizados destinados a proteger sistemas informáticos. Entonces, ¿su actuación contraviene el ordenamiento legal? No, pues, en este caso, se aplicaría el artículo 20.4 CP:

> **Art. 20 CP.-** 4. El que, ante un peligro actual e insuperable de otro modo, que amenace la vida, la integridad corporal, la libertad u otro bien jurídico, realiza un hecho destinado a conjurar dicho peligro de sí o de otro, siempre que concurran los siguientes requisitos:
>
> a) Cuando de la apreciación de los bienes jurídicos en conflicto afectados y de la intensidad del peligro que amenaza, el bien protegido resulta predominante sobre el interés dañado; y
>
> b) Cuando se emplee un medio adecuado para vencer el peligro.

Pongo a consideración del lector el siguiente análisis: (1) la brecha de seguridad advertida constituía un peligro actual, pues cualquier persona con conocimientos técnicos suficientes pudo acceder y cometer un atentado contra la integridad de los sistemas informáticos. Tanto es así, que Joaquín ingresó al sistema y tuvo la posibilidad de insertar datos en él. (2) Para comprobar la brecha de seguridad, Joaquín debía ingresar al sistema y realizar las acciones que efectuó, en consecuencia, no podía actuar de otro modo. (3) La amenaza era real y podía afectar el bien jurídico *seguridad informática* del gobierno argentino. (4) Garantizar la integridad del sistema informático prima sobre la vulneración de la confidencialidad o de los datos informáticos, en este caso concreto. (5) El medio empleado fue adecuado para vencer el peligro: Joaquín no alteró la configuración del sistema ni interfirió en su uso adecuado, de hecho, la acción que realizó (colocar una "bandera") es una práctica conocida y aceptada en el campo de la ciberseguridad.

Desde las primeras páginas de esta publicación, he sostenido que las actividades en el ciberespacio son tan interesantes y novedosas que nos llevan a replantearnos problemas sobre categorías jurídicas e instituciones tradicionales del derecho penal. He de reconocer que necesitamos profundizar nuestros estudios y que más investigadores se interesen en estos tópicos. En esta línea, en este libro busco nuevas respuestas para antiguos problemas.

Realizo esta reflexión, pues el caso que describiré a continuación reta las fronteras del ciberespacio y toca fibras muy sensibles por los difíciles momentos que estamos viviendo en Perú: ¿qué pasaría si una organización criminal secuestra a una persona y un grupo de *hackers* atenta contra datos y sistemas informáticos exigiendo su liberación? Quizás los ciudadanos no tengamos armas para defendernos, pero sí información y conocimiento que se puede divulgar en el ciberespacio.

[Caso 81] Los Zetas es un cártel de narcotráfico considerado como uno de los más poderosos y sanguinarios que han existido en México. En el 2011, esta organización criminal secuestró, en Veracruz, a un miembro de Anonymous[664], el cual es un grupo de *hacktivistas* de presencia mundial.

Como respuesta, el 6 de octubre, los ciberactivistas publicaron un video en el que exigieron la liberación de su *hermano anónimo*: "No podemos defendernos con armas. Pero podemos hacer esto con sus coches, casas, bares y todo lo que posean. No será difícil. Todos sabemos quiénes son y dónde están"[665].

Entre las acciones ejercidas por el grupo de *hacktivistas* se encuentra la intervención de la página web de Gustavo Rosario Torres, exfiscal de Tabasco. Así, el 28 de octubre de 2011, los atacantes reemplazaron su imagen por el siguiente mensaje: "Gustavo Rosario es Zeta"[666]. Como el lector puede intuir, nos encontramos frente a un ataque de *defacement*, esto es, alteración de datos informáticos.

664 Para conocer la importancia de sus operaciones, historia y filosofía, recomiendo: Coleman, Gabriella. *Las mil caras de Anonymous. Hackers, activistas, espías y bromistas*. Barcelona: Arpa y Alfil, 2016.

665 "México: Anonymous le declara la guerra a Los Zetas", en *BBC News Mundo*, 2 de noviembre de 2011. https://www.bbc.com/mundo/noticias/2011/11/111101_video_mexico_zetas_veracruz_anonymous_jg

666 "Showdown Looms Between 'Anonymous' Hackers and Mexico's Zeta Cartel", en *ABC NEWS*, 3 de noviembre de 2011. https://abcnews.go.com/International/showdown-looms-anonymous-hackers-mexicos-zeta-cartel/story?id=14875273

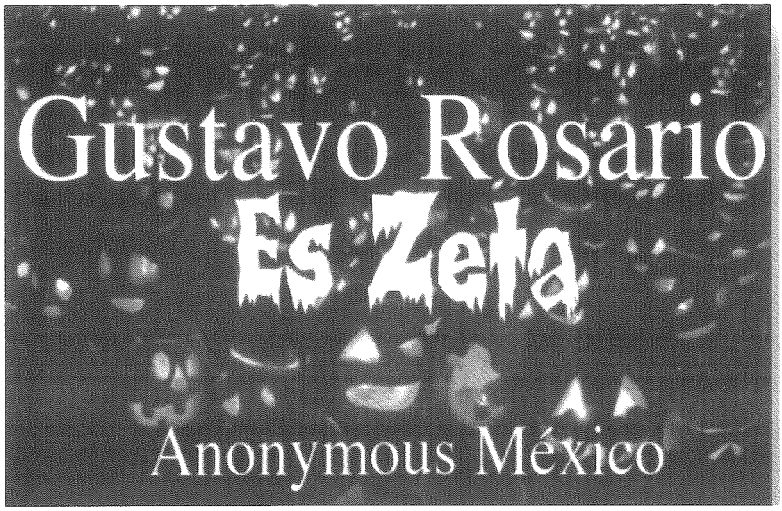


Imagen 19. La página web del exfiscal de Tabasco fue intervenida por Anonymous[667].

Tres días después, Anonymous reafirmó su intención de actuar. Así, el 31 de octubre de 2011, a través del blog Anonymous Iberoamérica[668], los ciberactivistas dieron a conocer públicamente su posición. Anunciaron que tomarían las precauciones necesarias para poner en marcha la denominada Operación Cártel -o #OpCartel-; no obstante, reconocieron los riesgos inherentes a la iniciativa y exhortaron a los miembros sin plena confianza en sus habilidades técnicas a no participar, advirtiendo que sus vidas podrían

667 La imagen fue obtenida en: URGENTE 24. *Anonymous carga contra el cártel de Los Zetas*, publicado el 1 de noviembre de 2011. https://urgente24.com/archivo/16463-anonymous-carga-contra-el-cartel-de-los-zetas Para conocer la importancia de sus operaciones, historia y filosofía, recomiendo: COLEMAN, Gabriella. *Las mil caras de Anonymous. Hackers, activistas, espías y bromistas*. Barcelona: Arpa y Alfil, 2016.
BBC News Mundo. *México: Anonymous le declara la guerra a Los Zetas*, publicado el 2 de noviembre de 2011. https://www.bbc.com/mundo/noticias/2011/11/111101_video_mexico_zetas_veracruz_anonymous_jg
ABC NEWS. *Showdown Looms Between 'Anonymous' Hackers and Mexico's Zeta Cartel*, publicado el 3 de noviembre de 2011. https://abcnews.go.com/International/showdown-looms-anonymous-hackers-mexicos-zeta-cartel/story?id=14875273
La imagen fue obtenida en: URGENTE 24. *Anonymous carga contra el cártel de Los Zetas*, publicado el 1 de noviembre de 2011. https://urgente24.com/archivo/16463-anonymous-carga-contra-el-cartel-de-los-zetas

668 Disponible en: https://anonopsibero.blogspot.com/2011/10/sobre-opcartel.html

estar en peligro. A continuación, se presenta un fragmento del comunicado difundido:

> [...] Debemos tener presente que estamos del lado del pueblo, y que no podemos dejar al pueblo de lado, sobre todo en momentos críticos como el que se vive actualmente. Además, si alguien efectúa una acción en nombre de Anonymous, los criminales no tendrán la perspicacia para distinguir quién desmintió o quién negó. Todo esto se veía venir y es inevitable. Estamos todos en el mismo buque, y seguiremos a flote, o nos hundiremos. No obstante, **recomendamos a todo aquel que no confíe lo suficiente en sus habilidades abstenerse de participar en esta operación**. Exhortamos a todo aquel que no esté correctamente protegido a deslindarse inmediatamente de esta operación, y hacerlo público, ya que es una operación extremadamente riesgosa en la que existe un peligro inminente y verosímil de pérdida de vidas humanas en cantidad. Nadie les tachará de cobardes, ni les acusará de abandonar a sus hermanos anónimos en lo más cruento de la batalla. Sabemos que muchos están deseosos de participar, pero les pedimos que lo reconsideren.
>
> ¿Tenemos miedo? Claro. ¿Tememos por nuestras vidas? Evidentemente. No obstante, creemos que es tiempo de decir alto y basta a la terrible situación provocada por la falsedad de los gobiernos y la falta de escrúpulos de personas a las que no les importa el bienestar de sus congéneres y han provocado una deplorable situación de ruina y desencanto en lugares como México, un país que se encuentra al borde del colapso, a solo pasos de una aniquilación total, por la necedad del gobierno en atacar los síntomas del problema y no sus causas, en aras de una situación de oligarquía de la que la gente se encuentra fastidiada.
>
> Nosotros seguiremos adelante con la operación, ya que así se nos ha solicitado. Para este fin, conformaremos una fuerza de tarea especial dedicada a este asunto. Sin embargo, requerimos de apoyo. ¿Cómo apoyar?
>
> - Si no estás correctamente protegido, abstente de participar, por muy emocionante que pienses que sea. ESTO NO ES UN VIDEOJUEGO. ES UNA OPERACIÓN RIESGOSA EN LA QUE PELIGRA TU VIDA Y LA DE LOS TUYOS.

- No te identifiques como Anónimo. Nunca debes hacerlo, pero en este momento menos. No uses fotos de perfil de Guy Fawkes ni portes la máscara en lugares públicos o de forma que se te pueda identificar.
- No adquieras máscaras de V por el momento, especialmente por correo.
- No asistas a demostraciones públicas con máscara de Anonymous ni hables de Anonymous a nadie.
- Hasta nuevo aviso, todos los Paperstorms y Citystorms quedan suspendidos.
- No te comprometas. Toda información relativa al narcotráfico háznosla llegar de forma anónima. Para este fin, hemos habilitado un *widget* para llevarlo a cabo. Envía tu denuncia y nuestro equipo especializado se encargará de ello, así como de darle difusión. No trates de hacerte el héroe.
- No existe forma de solicitar el ingreso a la fuerza de tarea especializada, así que no insistas. Únicamente existe por invitación.

Finalmente, Anonymous informó que su compañero fue liberado y que, en consecuencia, no continuarían con sus ataques cibernéticos. No obstante, los Zetas les enviaron un mensaje, a través de su compañero: por cada nombre del cártel revelado, diez personas serían asesinadas[669].

> En el día de hoy, nuestro compañero Anonymous retenido por el cártel de los zetas ha sido liberado.
>
> Hemos prestado sumo cuidado en verificar su identidad mediante contactos con sus compañeros y amigos y podemos decir que, aunque magullado, está sano y salvo.
>
> Nos ha hecho llegar un mensaje, si Anonymous desvela algún nombre relacionado con el cártel, la familia del anónimo retenido sufrirá las consecuencias, por cada nombre del cártel revelado, diez personas serán ajusticiadas.

669 Disponible en: https://anonopsibero.blogspot.com/2011/11/comunicado-opcartel.html

> No está en nuestro ánimo que la lucha diaria que llevamos a cabo por la libertad en el mundo conlleve que personas inocentes sean víctimas de la violencia y la barbarie que diariamente azotan a los mexicanos por parte de los cárteles de la droga.
>
> El colectivo de Anonymous ha decidido por consenso que la información de la que disponemos no sea desvelada por el momento, ya que entendemos que no podemos obviar las amenazas que involucran a personas civiles inocentes que nada tienen que ver con nuestras acciones.
>
> El Conocimiento es Libre
>
> Somos Anónimos.
>
> Somos Legión.
>
> No Perdonamos.
>
> No Olvidamos.
>
> Esperádnos.

Luego de analizar el caso, considero que, si bien el ataque a los datos afectó la seguridad informática del exfiscal de Tabasco, entre otros, lo cierto es que la actuación persiguió la liberación de uno de los integrantes de Anonymous. De este modo, si bien la conducta es típica, no sería antijurídica, porque se prefirió el bien jurídico *vida* y *salud* antes que la *seguridad informática* que les asiste a los agresores. Obviamente, nos encontramos frente a un caso polémico y, sobre el cual, necesitamos más información para adoptar una posición acabada.

6.10. CONSUMACIÓN

En Argentina, los tribunales precisaron que nos encontramos frente a un delito de resultado:

> El delito de daño informático (art. 183 CP), comprende dos tipos penales: 1) alterar, destruir o inutilizar datos, documentos, programas o sistemas informáticos; y 2) vender, distribuir, hacer circular o introducir en un sistema informático, cualquier programa destinado a causar daños. **Constituye delito de resultado, por lo que requiere para su**

> **consumación la comprobación del daño** que el dato, documento, programa o sistema informático han sufrido como consecuencia de la acción del sujeto activo y se trata de un delito doloso[670] [El resaltado es mío].

En la misma línea, la doctrina colombiana precisa que:

> Todo indica que el tipo penal de daño informático es de resultado *(in) material*, por lo cual es necesario verificar un *nexo lógico* cuando se trate de daños inmateriales sobre datos, componentes lógicos o sistemas de tratamiento de información, y un *nexo de causalidad* cuando el daño material recaiga sobre el sistema de tratamiento de información o sus partes. En el caso del nexo lógico es necesario determinar la existencia de una conexión virtual entre el usuario, el sistema informático y los datos. Dicho en otros términos, es fundamental probar la existencia de un diálogo informático entre el usuario o autor y el sistema informático que pueda producir un determinado daño, modificación, deterioro lógico a los datos y los sistemas informáticos (sus partes y componentes lógicos), según el propósito del autor, que consiste en la interacción *input-output* propiciada por las instrucciones electrónicas imputadas al sistema por el sujeto activo mediante el *hardware* y respondidas por la máquina[671].

Algunos autores locales consideran que ciertas modalidades de este delito -*dañar*, *introducir*, *alterar* y *deteriorar*- configuran actos de mera actividad y, en consecuencia, no admiten tentativa. En tanto, otras modalidades -*borrar*, *suprimir* y *hacer inaccesibles*- serían delitos de resultado que permiten la tentativa[672]. Otros no hacen esta distinción y sostiene que nos encontramos frente a

---

670 Pronunciamiento de la Sala I CCC 62182/2016/2/CFC1 "BA, F/recurso de casación", reg. 1859/21, rta. 12 de octubre de 2021. En: Poder Judicial de la nación de Argentina. *Ciberdelitos y evidencia digital*. Secretaria de Jurisprudencia. 2024, p. 8. https://mendozalegal.com/omeka/files/original/99099382dd28a7301f9bb5a885626b1a.pdf

671 Posada Maya, *Los cibercrímenes*, cit., p. 359.

672 Arévalo Minchola/Vega Aguilar, *Ciberdelitos. Análisis en el sistema penal*, cit., p. 282.

un delito de mera actividad, por la forma en cómo está redactado el tipo penal y las características de este ilícito[673].

Sobre el particular, he de indicar que el delito de atentado contra la integridad de los datos informáticos es un delito de resultado y en ese sentido deberán interpretarse o aplicarse los verbos rectores que el legislador peruano ha recogido. Ciertamente, uno de ellos generará problemas: introducir datos informáticos. Como he indicado anteriormente, este verbo no debería formar parte de este delito, ya que el Convenio de Budapest lo recoge como el medio para ocasionar otro delito (atentado contra la integridad o funcionamiento del sistema informático). Aplicando el *método de interpretación sistemática*[674] de las normas, recomiendo no utilizar este verbo rector al realizar una calificación jurídica, ya que generará problemas de subsunción. No obstante, recordemos que el elemento dañar es residual y cubre todo supuesto no previsto por el resto de las conductas.

6.11. CONCURSOS

Pareciera que un sector de la doctrina considera que este delito es el paso inmediato siguiente al acceso ilícito o que condiciona su configuración a la comisión previa del intrusismo informático: "El acto de destrucción o sabotaje viene precedido por un ingreso ilícito; no obstante, este ya queda consumido en el injusto de atentado a la integridad de datos informáticos"[675].

673 "Como vemos, en esta figura se exige el solo cumplimiento del tipo penal, la sola realización de la conducta tipificada para que se pueda configurar el ilícito, sin importar el resultado posterior. Eso quiere decir que efectos de la consumación no es necesario determinar si realmente se causó perjuicio a la víctima o, en su caso, establecer si el agente logró su objetivo de obtener su beneficio perseguido, tales aspectos serían irrelevantes" (Pérez López, *Delitos regulados en leyes penales especiales*, cit., p. 121).

674 "En resumen, el método sistemático por ubicación de la norma interpreta aplicando el conjunto de principios, conceptos, elementos y contenidos que sirven de "medio ambiente" a la norma dentro de su grupo o conjunto normativo. El método reposa en la concepción del Derecho como un sistema estructural y discrimina la interpretación en función de ello y no del "cuerpo legislativo" en el que se halla la norma jurídica [...]" (Rubio Correa, Marcial. *El sistema jurídico. Introducción al derecho.* Octava edición. Corregida y aumentada. Lima: Fondo Editorial de la Pontificia Universidad Católica del Perú, 1999, p. 271).

675 Oré Sosa, *Delictum. Apuntes de derecho penal*, cit., p. 195.

De la misma forma, se señala que "el delito de daño informático se configura cuando el agente ingresa indebidamente a una base de datos, con la finalidad de alterarla, dañarla o destruirla [...]. El grupo de conductas mencionado tiene en común dos características: en primer lugar, para su realización es necesario que, previamente, se haya producido un acceso ilícito a un sistema informático"[676].

Sobre este punto, debo señalar que existirán casos de atentados contra los datos informáticos en los que el agente previamente haya ingresado al sistema sin autorización e, incluso, vulnerando medidas de seguridad. No obstante, no es una condición, ya que muchos de estos ataques se producen sin el ingreso en referencia.

Cuando concurran los dos delitos secuencialmente (acceso ilícito y atentado contra la integridad de datos informáticos), como se sostuvo en el capítulo anterior, nos encontraremos frente a un *concurso ideal*, ya que estamos frente a una unidad de hecho típico.

[Caso 82] Puede ocurrir que se alteren datos informáticos con la finalidad de beneficiar a un tercero, por ejemplo, restarle puntos de infracción en el sistema de conducción y, de esta manera, rehabilitar al conductor. En este caso, nuestra Corte Suprema sostuvo que no nos encontramos frente a un concurso real de delitos (atentado contra datos y falsedad), sino uno ideal. En efecto, la Sala Penal Transitoria de la Corte Suprema de Justicia de la República emitió el Recurso de Nulidad N.º 805-2018, Lima, del 11 de abril de 2019.

> 7.3 Según la hipótesis fiscal [...], los procesados habrían incurrido en delito informático por haber ingresado indebidamente a la base de datos del Ministerio de Transportes y Comunicaciones (referido a la expedición de licencias de conducir), utilizando la información privilegiada (usuario y contraseña) que habrían recibido para el desempeño de sus funciones, para proporcionar información falsa a favor de su coprocesado Rubén Ángel Orosco Simeón, a cambio de un beneficio económico.

676 Pérez López, *Delitos regulados en leyes penales especiales*, cit., pp. 116 y s.

> 7.4 Sobre el delito de falsedad genérica, sostiene que los procesados alteraron la verdad intencionalmente en perjuicio del Ministerio de Transporte y Comunicaciones, a fin de que Rubén Ángel Orosco Simeón obtenga su licencia de conducir sin haber aprobado los exámenes de conocimiento de reglas y manejo.
>
> 7.5 Es claro que el supuesto de hecho es uno solo, advirtiéndose un concurso aparente de normas penales, el mismo que se presenta en aquellas situaciones en las que para la tipificación de un hecho concurren, en apariencia, dos o más tipos penales; sin embargo, una regla extraída del sistema jurídico permite determinar que el hecho se encuentra solo en uno de los supuestos típicos mencionados.
>
> 7.6 En efecto, la redacción del tipo penal de atentado contra la integridad de datos informáticos contempla varios verbos rectores como *introducir*, *borrar*, *deteriorar*, *alterar* y/o *suprimir datos informáticos falsos*. Expuesto así, se desprende que el hecho no se configura por la sola utilización del usuario y contraseña, sino que se debe alterar, introducir y/o modificar los datos informáticos, supuesto fáctico que también se les atribuye a los encausados como parte de los elementos objetivos del delito de falsedad genérica (alterar la verdad intencionalmente en perjuicio del Ministerio de Transporte y Comunicaciones); por lo que, **en aplicación del principio de especialidad, no cabe atribuir a los encausados dos conductas distintas respecto al mismo hecho que típicamente calza, por especialidad, en el delito informático** [El resaltado es mío].
>
> 7.7 En consecuencia, el hecho imputado se subsume, por resultar más específico, en la conducta descrita en el delito de atentado contra la integridad de datos informáticos y no en el de falsedad genérica, en tanto que el primer delito abarca la totalidad del hecho criminal, por tratarse de una norma especial.

Coincido con Ricardo Posadas en que una misma acción puede, con el paso del tiempo, generar resultados sucesivos. No obstante, en tales casos, estaríamos ante un delito único y no frente a un concurso homogéneo de tipos penales. Se trata, por tanto, de un supuesto de unidad típica de acción. Por ejemplo, imaginemos que un ciberdelincuente envía a su víctima un *malware* que encripta algunos archivos, altera el contenido de otros y destruye parte de

la información restante. En este escenario, estamos ante una sola acción que ha producido múltiples resultados lesivos[677].

6.12. PENALIDAD

En el delito de atentado a la integridad de datos informáticos, el autor es castigado con pena privativa de libertad no menos de tres ni más de seis años y con ochenta a ciento veinte días-multa.

Si comparamos la sanción impuesta por el acceso ilícito mediante la vulneración de medidas de seguridad con la establecida para los ataques contra la integridad de los datos informáticos, observamos que es exactamente la misma. Sin embargo, el legislador parece no distinguir que, en el intrusismo informático, no se afecta la disponibilidad ni la integridad de los datos, lo que hace que equiparar ambos delitos en términos de castigo resulte desproporcionado.

Lo mismo ocurre con los ataques a sistemas informáticos, ya que, en términos generales, estos generan un mayor perjuicio para el titular. Si bien pueden existir excepciones en las que el daño no sea significativo, en la mayoría de los casos, comprometer un sistema implica también afectar sus datos.

Por ello, considero que en ambos escenarios se presentan problemas de proporcionalidad en las sanciones establecidas por el legislador. En una eventual reforma legislativa, este debe ser un punto para debatir.

677 "Si las consecuencias nocivas de las conductas se prolongan en el tiempo, como cuando se utiliza un virus informático cuyo efecto dañino se concreta en el borrado de varios programas y archivos o la sobrecarga de los recursos del sistema, etc., en perjuicio de los mismos sistema y usuario durante un largo lapso, se tipifica solo un delito de daño informático, pues no es válido afirmar que cada vez que se causa un daño a un programa o archivo, por ejemplo, se tipifica un delito diferente, pues se trata de una sola conducta de daño, con independencia de la gravedad del mismo, que tendrá incidencia para los efectos de determinar el daño, dosificar la pena y cuantificar los perjuicios causados a la víctima" (Suárez Sánchez, Alberto. *Manual de delito informático en Colombia. Análisis dogmático de la ley 1273 de 2009*, Universidad del Externado, Bogotá, 2016, p. 277).

6.13. CIRCUNSTANCIAS AGRAVANTES

Le son aplicables las cinco circunstancias previstas en el artículo 11 de la Ley N.° 30096:

i) Cometer el delito como integrante de una organización criminal.

> **[Caso 83]** Wizard Spider es una ciberorganización criminal que ha dirigido sus ataques contra gobiernos, instituciones académicas, organizaciones sanitarias, manufactureras y tecnológicas. Este tipo de prácticas, esto es, atacar grandes empresas, es conocido como *big game hunting*. Se estima que, en el 2019, registro el mayor rescate solicitado: 12,5 millones de dólares y que, en el 2020, recaudó aproximadamente 150 millones[678].
>
> Se atribuye a Wizard Spider la distribución del *ransomware* Ryuk[679], cuyo nombre fue obtenido del manga *Death Note* y que significa 'regalo de Dios'. Para que este *malware* funcione, Ryuk deshabilita 180 servicios y 40 procesos. En ese instante, se procede a cifrar los datos informáticos -como fotografías, videos, bases de datos y documentos importantes- utilizando el algoritmo de encriptación AES-256.
>
> Es importante precisar que este *malware* ataca datos específicos, no encripta el sistema. De hacerlo, no lo analizaríamos como un supuesto del artículo 3 LDI, sino del artículo 4 LDI.

678 Trendmicro. *¿Qué es el ransomware RYUK?* https://www.trendmicro.com/es_mx/what-is/ransomware/ryuk-ransomware.html

679 En Perú, se ha encontrado referencias a este *ransomware* desde el 2021: Centro Nacional de Seguridad Digital. *Alerta integrada de seguridad digital N.° 47-2021*. Lima: 1 de marzo de 2021. https://www.gob.pe/institucion/pcm/informes-publicaciones/1733211-alerta-integrada-de-seguridad-digital-n-047-2021-pecert. "Ransomware Ryuk ahora se propaga automáticamente a otros dispositivos LAN de Windows". p. 12.Centro Nacional de Seguridad Digital. *Alerta integrada de seguridad digital N.° 94-2021*. Lima: 21 de abril de 2021. https://www.gob.pe/institucion/pcm/informes-publicaciones/1859225-alerta-integrada-de-seguridad-digital-n-094-2021-pecert. "Piratas informáticos del Ryuk Ransomware emplean RDP y otras técnicas de ataque". p. 4.

Una vez infectado el equipo, los atacantes dejan una nota de rescate similar a la siguiente imagen:

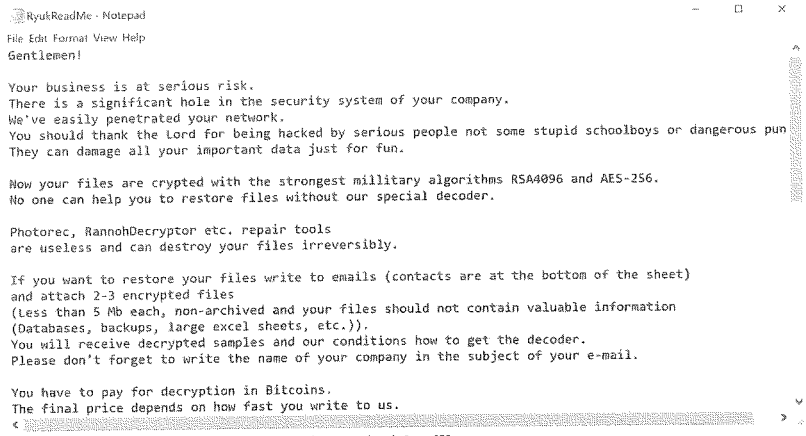


Imagen 20. Nota de rescate obtenida de Sentinel One[680].

ii) Cometer el delito mediante el abuso de una posición especial de acceso a la data o información reservada o al conocimiento de esta información en razón del ejercicio de un cargo o función. Como hemos visto en el capítulo anterior, esta modalidad se ejemplifica con los *insiders*, es decir, con aquellas personas que pertenecen a la institución o empresa víctima del ciberataque y que contribuyen activamente con el mismo. Así, por ejemplo, el *insider* podría llevar el *malware* en un USB, deshabilitar los antivirus e ingresarlo en algún dispositivo objetivo.

iii) Cometer el delito con la finalidad de obtener un beneficio económico.

[Caso 84] Hace 3 años, en el portal Reddit, un usuario posteaba: "Recomienden un *hacker* para cambiar mis notas"[681]. Lo que el usuario buscaba, en realidad, era un ciberdelincuente que

680 La imagen fue obtenida en: Sentinel One. *What is a Ryuk Ransomware? A Detailed Breakdown*, publicado el 16 de julio de 2021. https://www.sentinelone.com/cybersecurity-101/threat-intelligence/ryuk-ransomware/

681 La publicación se encuentra disponible en: https://www.reddit.com/r/PERU/comments/xck4y1/recomienden_un_hacker_para_cambiar_mis_notas

accediera al sistema de su institución y cambiara los datos informáticos (notas) que aparecen en el registro.

En el 2019, Kaspersky encontró que existen ciberdelincuentes que ofrecen tales servicios en línea. Así, descubrieron que en la *dark web* se ofrecían diversos servicios -desde alterar notas, hasta generar certificados o diplomas falsos-. Para ello, el interesado debía completar un formulario y dejar algunos datos de contacto[682].

Obviamente, quienes están detrás de este ilícito negocio no lo hacen con fines altruistas, sino que requieren un pago para alterar los datos informáticos.

iv) Comprometer fines asistenciales, la defensa, la seguridad y la soberanía nacionales. Si bien es posible atacar datos informáticos y, de este modo, poner en grave riesgo los objetivos descritos, es mucho más probable que esta modalidad se cometa a través del ataque a la integridad y la disponibilidad de los sistemas informáticos. No obstante, esta posibilidad queda abierta al análisis y aplicación.

v) Cometer el delito empleando la inteligencia artificial o tecnologías similares o análogas (conforme a la Ley N.º 32314).

6.14. PROPUESTA NORMATIVA

A partir del análisis expuesto en este capítulo, propongo modificar el delito de atentado a los datos informáticos, tomando en consideración:

i. Reformar el *nomen iuris* del delito actualmente denominado *atentado a la integridad de datos informáticos*, sustituyéndolo por *ataque a la integridad y disponibilidad de los datos informáticos.*
ii. Eliminar los elementos *deliberada* e *ilegítimamente.*
iii. Eliminar el verbo rector *introducir.*

682 Jacoby, David. "El mercado negro de los certificados académicos", en *Kaspersky Daily*, 24 de julio de 2019. https://www.kaspersky.es/blog/school-hacking/18736/?srsltid=AfmBOop4hGsJAbqd-J8MK_JqLfRUZa-A3Bh3wXeygi1qF_MiqKSh9-G9

iv. Incluir la *gravedad* del daño como elemento objetivo del tipo.
v. Modificar la sanción prevista, en atención a la gravedad que representa.

De este modo, el delito bajo estudio se regularía en los siguientes términos:

> Art. 3.- Ataque a la integridad y disponibilidad de los datos informáticos
>
> El que daña, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, cuando el resultado producido sea grave, será reprimido con pena privativa de libertad no menor de cuatro ni mayor de ocho años y con ochenta a ciento veinte días-multa.

6.15. CONCLUSIONES DEL CAPÍTULO

- El sexto capítulo aborda el delito denominado *atentado contra la integridad de los datos informáticos*, considerado una manifestación de los daños informáticos. Se explica que este delito se diferencia del daño a sistemas informáticos y se ejemplifica con dos casos históricos relevantes: el de Donald Burleson, en 1988, y el ataque global NotPetya, en 2017, que demuestran el rango de afectación que puede tener este delito, desde daños personales hasta impactos globales.
- El Convenio de Budapest, en su artículo 4, establece una tipificación clara del delito, sancionando conductas como *dañar*, *borrar*, *deteriorar*, *alterar* o *suprimir datos informáticos*. También contempla la posibilidad de exigir que estos actos conlleven un daño grave. En este capítulo, se destaca cómo esta norma busca proteger no solo la integridad, sino también la disponibilidad de los datos informáticos, entendidos como objetos jurídicos intangibles, equiparables a bienes corpóreos ante ataques dolosos.
- Por su parte, la Convención de las Naciones Unidas contra la Ciberdelincuencia también recoge la figura delictiva bajo el nombre de *interferencia con datos electrónicos*, en términos prácticamente idénticos al Convenio de Budapest. A pesar de las diferencias terminológicas, ambas normas internacionales apuntan a una protección penal robusta frente a la destrucción o deterioro de los datos.

- El análisis de la legislación comparada en América Latina revela diferencias sustanciales en la tipificación del delito, tanto en el *nomen iuris* como en los verbos rectores empleados. Mientras algunos países como Chile y España exigen un daño grave para su configuración, otros, como Perú, no introducen tal exigencia. Asimismo, se advierte que algunos ordenamientos han incorporado acciones no sugeridas por los instrumentos internacionales, como *introducir*, *hacer inaccesible*, *copiar* o *mutilar*, lo que genera inseguridad jurídica y problemas en la interpretación y aplicación.
- En el Perú, el delito fue incorporado por primera vez en el año 2000 y reformulado por la Ley de Delitos Informáticos. La versión actual castiga a quien, de forma deliberada e ilegítima, dañe, introduzca, borre, deteriore, altere, suprima o haga inaccesibles datos informáticos. A diferencia de otros delitos, no se exige un resultado de gravedad para su configuración, lo que plantea críticas desde el principio de lesividad y proporcionalidad penal.
- La inclusión del verbo rector *introducir* carece de justificación; es más, podría generar confusión. Por ejemplo, la conducta de introducir datos maliciosos afecta, en realidad, el funcionamiento de los sistemas informáticos antes que a los datos en sí. Aunado a esto, estos verbos no figuran en el Convenio de Budapest que sirvió de base para nuestra legislación actual.
- En cuanto al bien jurídico protegido, el delito analizado no tutela el patrimonio en sentido estricto, como ocurre en algunos ordenamientos, sino la seguridad informática, entendida como la integridad y disponibilidad de los datos. Se descarta que el objeto de protección sea la confidencialidad -relevante en otros delitos informáticos como el intrusismo o la interceptación- o el patrimonio digital, ya que este enfoque podría derivar en una errónea tipificación como delito patrimonial.
- Este delito es común, es decir, puede ser cometido por cualquier persona, incluso sin conocimientos técnicos avanzados, dadas las herramientas disponibles en internet y otros medios. El sujeto pasivo es quien ostenta la titularidad de los datos informáticos, sean personas naturales o jurídicas.

- Respecto a la tipicidad objetiva, en este capítulo se analizan uno a uno los verbos rectores recogidos en la legislación peruana. Se destaca que cada uno presenta diferentes niveles de afectación y debe ser interpretado con precisión. Por ejemplo, *borrar* implica una destrucción definitiva de los datos, mientras que *deteriorar* alude a una merma en su funcionalidad. *Dañar* es un término residual que cubre cualquier conducta que cause perjuicio no tipificada expresamente en las otras modalidades.
- Finalmente, en este capítulo se enfatiza la necesidad de revisar y actualizar la redacción del tipo penal en el Perú, proponiendo una mayor armonización con la legislación comparada, una delimitación mucho más precisa de los verbos rectores y la incorporación del criterio de *gravedad* como elemento objetivo del tipo. Esto permitiría evitar la criminalización de conductas de escasa lesividad y otorgaría mayor coherencia y eficacia a la protección penal de los datos informáticos.

CAPÍTULO 7

ATENTADO A LA INTEGRIDAD DE SISTEMAS INFORMÁTICOS



* La ilustración de la página anterior corresponde a una adaptación de *Calle de París, tiempo lluvioso*, de Gustave Caillebotte (1877). Para su elaboración, se empleó una de las herramientas de generación de imágenes de la empresa OpenAI.

CAPÍTULO 7

ATENTADO A LA INTEGRIDAD DE SISTEMAS INFORMÁTICOS

Sumario: 7.1. Introducción. 7.2. Regulación en el Convenio sobre la Ciberdelincuencia. 7.3. Regulación en la Convención de las Naciones Unidas contra la Ciberdelincuencia. 7.4. Legislación comparada. 7.5. Legislación nacional. 7.6. El bien jurídico penalmente protegido. 7.7. Tipicidad objetiva. 7.8. Tipicidad subjetiva. 7.9. Las situaciones de justificación en el delito de atentado a la integridad de sistemas informáticos. 7.10. Consumación. 7.11. Concursos. 7.12. Penalidad. 7.13. Circunstancias agravantes. 7.14. Propuesta normativa. 7.15. Conclusiones del capítulo.

Ooops, your files have been encrypted!

What happened to my computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recovery your files without your decryption service.

Can I recover my files?

Sure. We guarantee that you can recover all files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recovery your files forever.

> We will have free events for users who are so poor that they couldn't pay in 6 months.
>
> **How do I pay?**
>
> Payment is accepted in Bitcoin only [...][683]

7.1. INTRODUCCIÓN

El delito que analizaremos en este capítulo es una manifestación del *sabotaje informático* (*computer sabotage*). A diferencia del ilícito previamente analizado, la tipificación peruana del atentado contra la integridad de los sistemas informáticos difiere sustancialmente de lo propuesto en el Convenio de Budapest. Así, el legislador local no exige la *obstaculización grave* del funcionamiento del sistema informático, tampoco establece que es el resultado de la introducción, daño, borrado, deterioro, alteración o supresión de datos informáticos.

Como se explicará en este apartado, el legislador peruano optó por omitir cualquier mención a los datos informáticos en la redacción de este delito, omitir el elemento *gravedad* y reemplazar el verbo *obstaculizar* por *inutilizar*, *impedir el acceso*, *entorpecer*, *imposibilitar* el funcionamiento del sistema informático o la prestación de sus servicios.

Antes de iniciar, abordaré algunos casos que ocurrieron en la red social X, antes Twitter, que grafican el impacto de los ciberataques y sus consecuencias sobre la empresa, sus titulares y eventuales víctimas. Estos ejemplos, además, nos permitirán diferenciar los ataques contra los datos y contra los sistemas informáticos.

[Caso 85] En junio de 2020, la periodista Juliana Oxenford sufrió el hackeo de su cuenta de Twitter, esto es, alguien ingresó a su cuenta, cambió

683 Mensaje emergente que aparecía en el dispositivo de la víctima de un ataque de ransomware del tipo Wanna Cry. "El ransomware Wanna Cry, que significa "quiero encriptar", "quiero llorar", "quiero cifrar", atacó 230 000 sistemas en 150 países. Wanna Cry se creó sobre la base de una herramienta robada a la NSA llamada Eternal Blue que explota vulnerabilidades de Windows, y Microsoft, fabricante del sistema operativo de Windows, ya había alertado sobre esta vulnerabilidad" (Dupuy, Daniela. "Ciberdelitos. Desafíos para trabajar". En: Ferrazzuolo, Vanessa Y. [coord.]. *Era digital: delito y prevención*. Buenos Aires: Jusbaires, 2019, p. 141).

las credenciales e impidió que volviera a entrar. Sin duda, el impacto fue enorme, ya que la periodista sumaba más de dos millones de seguidores[684].

Cinco años después, otra periodista peruana muy influyente, Rosa María Palacios, reportó un caso similar. Con casi cuatro millones de seguidores, la cuenta fue vulnerada y utilizada para ofrecer inversiones en criptomonedas -claramente, un caso de estafa en contra de sus seguidores-. Felizmente, la abogada y periodista pudo recuperar su cuenta no sin antes dejar este mensaje en su columna semanal:

> Como todo sucede junto, el viernes me robaron mi cuenta de X, con 3.770.000 seguidores, haciéndose pasar como la propia plataforma. Un bocado apetitoso porque el ladrón cambió mi correo asignado y mi teléfono y logró poner propaganda de horrorosas criptomonedas. Todavía no la recupero, pero no es una tragedia. Tragedia es atravesar un puente que se cae o estar en un centro comercial y que el techo te mate. Y lo peor de todo, sabiendo con pasmosa resignación que tus deudos no van a encontrar reparación. Esa es la verdadera tragedia[685].

Estos dos casos reflejan a lo que todos estamos expuestos, independientemente del número de nuestros seguidores. Sin embargo, aun cuando el usuario no puede acceder a la plataforma, no nos encontramos frente a un ataque contra la integridad o la disponibilidad del sistema -ya que este se mantiene incólume-, sino contra los datos informáticos.

El caso que se analiza a continuación grafica cómo se produce este tipo de ataques, pues, muchas veces, se encuentran organizados o, por lo menos, coordinados.

---

684 "Juliana Oxenford tras ser hackeada por segunda vez en Twitter: La idea es anularme de todas las redes sociales", en *Peru21*, Lima, 15 de junio de 2020. https://peru21.pe/espectaculos/juliana-oxenford-tras-ser-hackeada-por-segunda-vez-en-twitter-la-idea-es-anularme-de-todas-las-redes-sociales-la-beba-army-nndc-nnes-noticia/

685 Palacios, Rosa María. "Me robaron mi cuenta en X", en *La República*, Lima, 23 de febrero de 2025. https://larepublica.pe/opinion/2025/02/23/me-robaron-mi-cuenta-en-x-por-rosa-maria-palacios-307602

[Caso 86] En noviembre del 2024, la compañía de ciberseguridad Bitdefender identificó una campaña global de publicidad maliciosa que aprovechó los anuncios difundidos a través de Facebook. De esta forma, los delincuentes distribuyeron el *malware* SYS01, el cual buscaba recopilar las credenciales de los usuarios y secuestrar sus cuentas.

Los anuncios engañaron a los usuarios para que descargaran contenido malicioso disfrazado como archivos legítimos, suplantando páginas web para dar apariencia de veracidad[686]. Una vez descargado e instalado, el *malware* robaba datos sensibles como *cookies* del navegador, credenciales guardadas, historial de navegación, entre otros. Así, se extrajo información del perfil del usuario (como nombre, correo electrónico, fecha de cumpleaños), se recabaron datos detallados de cuentas publicitarias, lo que incluyó gastos efectuados y métodos de pago, cuentas publicitarias, usuarios profesionales, agencias, etcétera.

El objetivo de los ciberdelincuentes era apropiarse de cuentas de Facebook, principalmente, de índole comercial[687].

686 A través de la publicidad se ofrece descargar programas como CapCut, herramientas de productividad como Office 365, servicios de *streaming* como Netflix e, incluso, videojuegos.

687 Centro Nacional de Seguridad Digital. *Alerta integrada de seguridad digital* N.º 255-2024. Lima: 5 de noviembre de 2024, p. 4. https://www.gob.pe/institucion/pcm/informes-publicaciones/6150042-alerta-integrada-de-seguridad-digital-n-255-2024-cnsd
Véase, además: "Descubren publicidad maliciosa en Facebook que difunde malware para robar información y secuestrar cuentas", en *Infobae*, 17 de julio de 2024. https://www.infobae.com/america/agencias/2024/07/17/descubren-publicidad-maliciosa-en-facebook-que-difunde-malware-para-robar-informacion-y-secuestrar-cuentas/

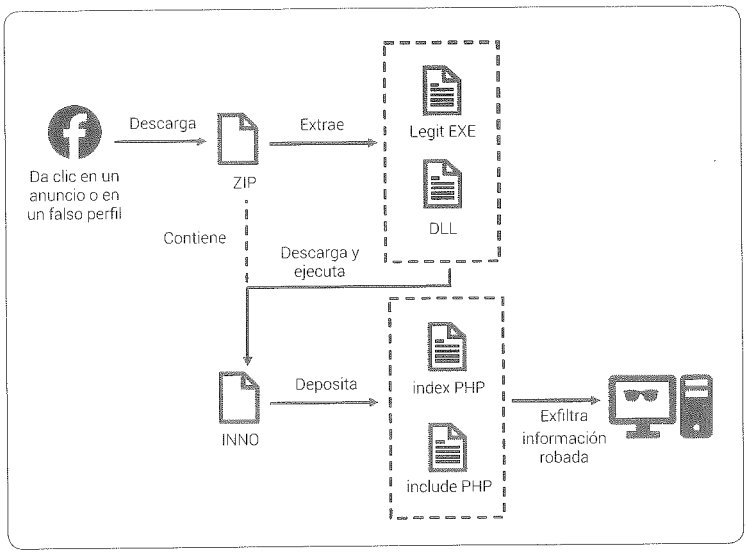


Diagrama 13. Estructura del *malware* SYS01. Adaptación [688].

[**Caso 87**] Como veremos a continuación, los ciberdelincuentes no solo atacan cuentas de *influencers*, sino también de entidades estatales. El 22 de noviembre de 2024, la Biblioteca Nacional del Perú fue víctima de un ciberataque[689] dirigido contra su cuenta en la red social X, en la que reunía más de treinta mil seguidores. El ataque originó que la institución perdiera el acceso y que, algunos días después, se emitiera el siguiente comunicado:

> Lamentamos informar que nuestra cuenta oficial de X ha sido víctima de un ataque cibernético. El incidente fue detectado hoy miércoles 27 de noviembre de 2024 y estamos tomando medidas inmediatas para superar el incidente.

688 Morphisec. *How SYS01 Stealer Will Get Your Sensitive Facebook Info*, publicada el 7 de marzo de 2023. https://www.morphisec.com/blog/sys01stealer-facebook-info-stealer/

689 Centro Nacional de Seguridad Digital. *Alerta integrada de seguridad digital N.º 274-2024*. Lima: 27 de noviembre de 2024, p. 4. https://www.gob.pe/institucion/pcm/informes-publicaciones/6240167-alerta-integrada-de-seguridad-digital-n-274-2024-cnsd

> Nos encontramos trabajando para recuperar el control de nuestra cuenta. Por ello, les pedimos no difundir cualquier mensaje o publicación emitida desde nuestra cuenta X.
>
> Les mantendremos informados a través de nuestros canales oficiales de Facebook, Instagram, TikTok y LinkedIn, así como de nuestra sede digital.
>
> Desde la Biblioteca Nacional del Perú reiteramos nuestro compromiso con la transparencia y la seguridad de la información[690].

Hasta fines de marzo del 2025, al parecer, la institución no pudo recuperar el acceso a dicha red social, pues la última actividad que reporta son dos reposteos -o republicaciones- de contenido erótico -uno de los cuales, tiene un enlace (posiblemente) malicioso-. Los atacantes no han eliminado el contenido previo, pero sí han cambiado el banner, la descripción de la cuenta, la imagen y el nombre de usuario, reemplazándolo por @peruporn69.



Imagen 21. Último tuit publicado en la cuenta de la Biblioteca Nacional del Perú, el 22 de noviembre de 2024 [691].

690 El comunicado ha sido descargado de *La República*: "Hackeo a la Biblioteca Nacional del Perú afecta su cuenta de X con mensajes indeseados", Lima, 28 de noviembre de 2024. https://larepublica.pe/sociedad/2024/11/27/ataque-cibernetico-a-la-biblioteca-nacional-del-peru-compromete-su-cuenta-de-x-con-contenido-inapropiado-noticias-1703187

691 Disponible en: https://x.com/peruporn69/status/1860097155039649960?s=46&t=9ZyXXlqVOPetmrOcFY3rZw

Los ejemplos descritos hasta este punto son manifestaciones de atentados contra la integridad o disponibilidad de datos informáticos -no olvidar que, según la LDI y el Convenio de Budapest, los programas integran este concepto-. A continuación, veremos un caso de ataque contra sistemas informáticos.

[Caso 88] A inicios del 2025, la plataforma X -antes Twitter-, propiedad de Elon Musk, sumaba más de 500 millones de usuarios activos. El 10 de marzo, durante varias horas, el *timeline* no se actualizaba y sus usuarios no podían utilizar sus cuentas: la plataforma se había *caído* producto de un ciberataque.

Pocos días después, The Dark Storm Team se atribuyó el ataque de denegación de servicio dirigido contra la referida plataforma. Sobre el particular, el Chief Technologist Oded Vanunu declaró que:

> El resurgimiento de The Dark Storm Team destaca la creciente amenaza contra plataformas *online* e infraestructuras críticas. Para los usuarios, esto implica posibles interrupciones, tiempos de inactividad y acceso limitado a servicios esenciales. Mientras las empresas trabajan para mitigar estos ataques, los usuarios pueden experimentar retrasos o errores en plataformas afectadas[692].

692 "The Dark Storm Team se atribuye ataque DDoS contra X (Twitter)", en *trendTIC*, 13 de marzo de 2025. https://www.trendtic.cl/2025/03/the-dark-storm-team-se-atribuye-ataque-ddos-contra-x-twitter/
En la misma línea: "Un grupo de ciberdelincuentes propalestino se atribuye los ataques que interrumpieron el servicio de X", en *El País*, 11 de marzo de 2025. https://elpais.com/tecnologia/2025-03-11/un-grupo-de-ciberdelincuentes-propalestino-se-atribuye-los-ataques-que-interrumpieron-el-servicio-de-x.html

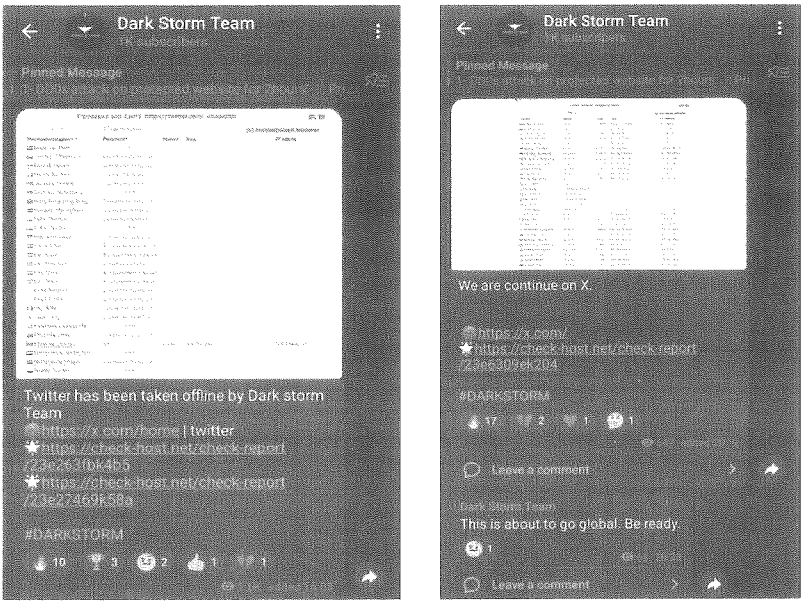


Imagen 22. Mensajes de ataque posteados en el canal de Telegram de Dark Storm Team[693].

Si bien los ciberataques que hemos visto hasta este punto tienen una característica común -el usuario que no puede acceder a su cuenta-, el modo y la afectación son distintos: de un lado, la vulneración de medidas de seguridad y la alteración de datos de ingreso de un usuario y, de otro, el ataque de DDoS contra el sistema que afectan a millones.

[Caso 89] Los ciberataques contra sistemas informáticos no afectan únicamente a empresas o instituciones gubernamentales. En noviembre de 2024, el Colegio de Abogados de Lima sufrió un ataque de secuestro informático que se hizo público recién en febrero del año siguiente. El objetivo habría sido la base de datos de los agremiados:

> El Colegio de Abogados de Lima informa a la comunidad jurídica que, en noviembre de 2024, un ataque de *ransomware* comprometió momentáneamente la operatividad de dos servidores institucionales. No obstante, la labor institucional no se vio interrumpida, y se tomaron medidas inmediatas, las cuales se detallan:

693 La imagen fue descargada de la publicación previamente referenciada.

1. Recuperación y resguardo de bases de datos: se han desplegado esfuerzos para restaurar la información afectada y reforzar las copias de seguridad física y virtual.
2. Fortalecimiento de la ciberseguridad institucional: se han implementado medidas avanzadas de protección, como el uso de autenticación de dos factores, encriptación de datos y la instalación del sistema de detección y respuesta ante amenazas (EDR) de Fortinet.
3. Seguridad perimetral y monitoreo continuo: se han actualizado los antivirus corporativos, configurado *firewalls* y segmentado la red para reducir riesgos, asegurando un monitoreo constante ante posibles amenazas.
4. Conformación de una comisión especializada: se ha designado una comisión integrada por la Dirección de Comunicaciones e Informática Jurídica, Dirección de Defensa Gremial y la Secretaría General para que determine la existencia de daños, la recuperación de la información y se indique, de ser el caso, quiénes son los responsables por acción u omisión.

Estas acciones se desarrollan sin perjuicio de la denuncia interpuesta por la Dirección de Defensa Gremial en el marco de la normativa vigente sobre delitos informáticos.

Finalmente, la Dirección de Comunicaciones e Informática Jurídica ha remitido un informe al respecto a Secretaría General con copia a la Oficina de Personal del CAL a fin que se tomen acciones por no haberse generado copias de seguridad (*backup*)[694].

Poco tiempo después, el Ministerio de Justicia y Derechos Humanos realizó acciones de fiscalización, a través de la Autoridad Nacional de Protección de Datos Personales[695]. Según la información difundida en canales guber-

694 Comunicado N.º 014-2025/CAL del 12 de febrero de 2015: "CAL informa sobre medidas implementadas para la protección de datos y cyberseguridad", Lima, 12 de febrero de 2015. https://www.cal.org.pe/v1/2025/02/13/cal-informa-sobre-medidas-implementadas-para-la-proteccion-de-datos-y-ciberseguridad/

695 Ministerio de Justicia y Derechos Humanos. *MINJUSDH realiza acciones de fiscalización al Colegio de Abogados de Lima por ataque cibernético a su base de datos y denuncia de agremiada*, publicado el 13 de marzo de 2025. https://www.gob.pe/institucion/minjus/noticias/1125784-minjusdh-realiza-acciones-de-fiscalizacion-

namentales, se realizaron dos visitas, el 25 de febrero y el 10 de marzo, respectivamente, con la finalidad de constatar las medidas de seguridad implementadas por el Colegio de Abogados de Lima.

Los ejemplos con los que iniciamos este capítulo evidencian la importancia del impacto y el daño que puede generar los ataques contra la integridad y la disponibilidad de los datos y sistemas informáticos.

7.2. Regulación en el Convenio sobre la Ciberdelincuencia

El delito de atentado o ataque a la integridad de sistemas informáticos se encuentra previsto en el artículo 5 del Convenio sobre la Ciberdelincuencia y se encuentra redactado en los siguientes términos:

> **Art. 5.- Ataques a la integridad del sistema**
>
> Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.

El delito bajo análisis puede graficarse de la siguiente forma:

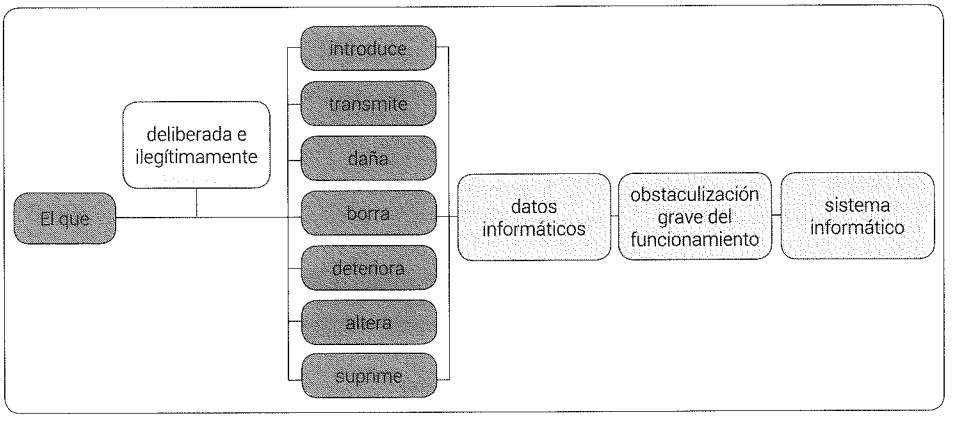


Diagrama 14. Estructura del delito de ataque a la integridad del sistema, propuesto en el Convenio de Budapest. Elaboración propia.

al-colegio-de-abogados-de-lima-por-ataque-cibernetico-a-su-base-de-datos-y-denuncia-de-agremiada

Los párrafos 65 a 70 del Informe Explicativo del Convenio de Budapest describen las razones de su criminalización y nos brindan algunas luces que permiten comprender sus alcances y límites:

- El párrafo 65 es muy claro al recordarnos que nos encontramos frente a sabotajes informáticos dirigidos a obstaculizar el uso de sistemas informáticos -incluyendo los servicios de telecomunicaciones-. Así, se recuerda que existe preocupación jurídicamente relevante en la protección del "interés de los operadores y los usuarios de los sistemas informáticos o de telecomunicaciones en su funcionamiento correcto". Se agrega que la redacción de este tipo penal emplea un "lenguaje neutral" para proteger todo tipo de funciones.
- En el párrafo 66 del Informe Explicativo se define la *obstaculización*, de manera amplia, como "las acciones que interfieren con el correcto funcionamiento de un sistema informático", precisándose que dicha obstaculización debe originarse en la introducción, transmisión, daño, borrado, alteración o supresión de datos informáticos. La legislación peruana se aleja de esta fórmula típica.
- El párrafo 67 destaca que la obstaculización debe ser *grave* -exigencia que no ha sido adoptada en nuestro país-. De este modo, se indica que las partes podrán exigir que se haya causado un mínimo de daños para que la obstaculización sea considerada relevante penalmente. Así, se considera grave, el envío de datos a un sistema cuando su forma, tamaño o frecuencia produzca un efecto perjudicial significativo en la capacidad que tiene el usuario para utilizar el sistema o comunicarse con otros. Esto sucede, por ejemplo, en los ataques de denegación de servicio.
- El párrafo 68 indica que no se consideran conductas ilegítimas o antijurídicas las actividades inherentes al diseño de las redes o las prácticas comerciales y de operación comunes: verificación de la seguridad de un sistema informático, su protección o reconfiguración, autorizado por su titular -claro está-.
- El párrafo 69 hace referencia al envío de correos electrónicos no solicitados, denominado *bombardeo publicitario* o *spamming*. De manera acertada, se señala que, en ciertas ocasiones, la agresividad

(por la cantidad y la frecuencia) podría generar un perjuicio grave en su receptor. Por esto, deja que cada parte analice en qué contextos podría configurar un delito y en qué circunstancias una falta de índole administrativo.

- Finalmente, el párrafo 70 recuerda que la conducta ilícita debe ser deliberada. Como he adelantado, Perú agregó este elemento subjetivo en la redacción del tipo penal.

7.3. REGULACIÓN EN LA CONVENCIÓN DE LAS NACIONES UNIDAS CONTRA LA CIBERDELINCUENCIA

El artículo 10 de la Convención regula el delito de interferencia con un sistema de tecnología de la información y comunicación en los siguientes términos:

> **Art. 10.- Interferencia con un sistema de tecnología de la información y comunicación**
> Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para tipificar como delito en su derecho interno la obstaculización grave, deliberada y sin derecho del funcionamiento de un sistema de tecnología de la información y la comunicación mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos electrónicos.

Como se puede apreciar, la opción legislativa es similar al Convenio de Budapest, en tanto prevé una obstaculización grave del funcionamiento de un sistema que es causado por siete tipos de acciones: introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos electrónicos. A diferencia del Convenio y de la LDI, no emplea la expresión *sistemas informáticos*, sino *sistemas de la información y la comunicación*. No obstante, su definición es casi idéntica:

> Todo dispositivo o conjunto de dispositivos interconectados o relacionados entre sí cuya función, o la de algunos de sus elementos, sea reunir, almacenar y procesar automáticamente datos electrónicos mediante la ejecución de un programa (art. 2, Convención de las Naciones Unidas contra la Ciberdelincuencia).

7.4. Legislación comparada

País	Legislación	Tipo penal
Países latinoamericanos que se adhirieron al Convenio de Budapest		
Ecuador	**Código Orgánico Integral Penal**	**Sección Tercera. Delitos contra la seguridad de los activos de los sistemas de la información y comunicación** **Art. 232.- Ataque a la integridad de sistemas informáticos** La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento o comportamiento no deseado, o suprima total o parcialmente [...] sistemas informáticos, sistemas de tecnologías de información y comunicación, dispositivos electrónicos o infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general, con el propósito de obstaculizar de forma grave, deliberada e ilegítima el funcionamiento de un sistema informático, será sancionada con pena privativa de libertad de tres a cinco años. [...] Si la infracción se comete sobre bienes informáticos, destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad.
Brasil	**Código Penal**	**Capítulo II. Dos crimes contra a segurança dos meios de comunicação e transporte e outros serviços publicos** **Art. 266.- Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública** Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento: Pena - detenção, de um a três anos, e multa. 1. Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.
Colombia	**Código Penal**	**Título VII-A. De delitos contra el patrimonio cultural sumergido** **Art. 269 D.- Daño informático** El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima [...] un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.
Paraguay	**Código Penal**	**Capítulo II. Hechos punibles contra otros derechos patrimoniales** **Art. 175.- Sabotaje de computadoras** 1. El que obstaculizara un procesamiento de datos de un particular, de una empresa, asociación o de una entidad de la administración pública, mediante: 1. Un hecho punible según el Art. 174, inciso 1°; o 2. La destrucción, inutilización, sustracción o alteración de una instalación de procesamiento de datos, de una unidad de almacenamiento o de otra de sus partes componentes indispensable. Será castigado con pena privativa de libertad de hasta cinco años o con multa. 2. En estos casos será castigada también la tentativa.
Argentina	**Ley N.° 11179**	**Capítulo VII. Daños** **Art. 183.-** Será reprimido con prisión de quince días a un año, el que destruyere, inutilizare, hiciere desaparecer o de cualquier modo dañare una cosa mueble o inmueble o un animal, total o parcialmente ajeno, siempre que el hecho no constituya otro delito más severamente penado. En la misma pena incurrirá el que alterare, destruyere o inutilizare [...] sistemas informáticos [...] o introdujere en un sistema informático cualquier programa destinado a causar daños.

País	Legislación	Tipo penal
Costa Rica	Código Penal	**Sección VII. Daños** **Art. 229 *ter*.- Sabotaje informático** Se impondrá pena de prisión de tres a seis años al que, en provecho propio o de un tercero, destruya, altere, entorpezca o inutilice la información contenida en una base de datos, o bien, impida, altere, obstaculice o modifique sin autorización el funcionamiento de un sistema de tratamiento de información, sus partes o componentes físicos o lógicos, o un sistema informático. La pena será de cuatro a ocho años de prisión cuando: a) Como consecuencia de la conducta del autor sobrevenga peligro colectivo o daño social. b) La conducta se realice por parte de un empleado encargado de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tenga acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos. c) El sistema informático sea de carácter público o la información esté contenida en bases de datos públicas. d) Sin estar facultado, emplee medios tecnológicos que impidan a personas autorizadas el acceso lícito de los sistemas o redes de telecomunicaciones.
Chile	Ley N.° 21459	**Título I. De los delitos informáticos y sus sanciones** **Art. 1.- Ataque a la integridad de un sistema informático** El que obstaculice o impida el normal funcionamiento, total o parcial, de un sistema informático, a través de la introducción, transmisión, daño, deterioro, alteración o supresión de los datos informáticos, será castigado con la pena de presidio menor en sus grados medio a máximo.
Panamá	Código Penal	**Título I. De los delitos informáticos y sus sanciones** No se ha encontrado una norma similar en el Capítulo I - "Delitos contra la seguridad informática" del Título VIII-Delitos contra la Seguridad Jurídica de los Medios Electrónicos del Código Penal.
República Dominicana	Ley N.° 53-07	**Capítulo I. Crímenes y delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos** **Art. 11.- Sabotaje** El hecho de alterar, maltratar, trabar, inutilizar, causar mal funcionamiento, dañar o destruir un sistema electrónico, informático, telemático o de telecomunicaciones, o de los programas y operaciones lógicas que lo rigen, se sancionará con las penas de tres meses a dos años de prisión y multa desde tres hasta quinientas veces el salario mínimo.
Otras referencias		
España	Código Penal	**Capítulo IX. De los daños** **Art. 264** *bis*.- 1. Será castigado con la pena de prisión de seis meses a tres años el que, sin estar autorizado y de manera grave, obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno: a) realizando alguna de las conductas a que se refiere el art. anterior; b) introduciendo o transmitiendo datos; o c) destruyendo, dañando, inutilizando, eliminando o sustituyendo un sistema informático, telemático o de almacenamiento de información electrónica. Si los hechos hubieran perjudicado de forma relevante la actividad normal de una empresa, negocio o de una administración pública, se impondrá la pena en su mitad superior, pudiéndose alcanzar la pena superior en grado. 2. Se impondrá una pena de prisión de tres a ocho años y multa del triplo al décuplo del perjuicio ocasionado, cuando en los hechos a que se refiere el apartado anterior hubiera concurrido alguna de las circunstancias del apartado 2 del art. anterior. 3. Las penas previstas en los apartados anteriores se impondrán, en sus respectivos casos, en su mitad superior, cuando los hechos se hubieran cometido mediante la utilización ilícita de datos personales de otra persona para facilitarse el acceso al sistema informático o para ganarse la confianza de un tercero.

Cuadro 23. Legislación comparada respecto al delito de atentado a la integridad de sistemas informáticos. Elaboración propia.

Algunas legislaciones analizadas -como las de Argentina, Colombia, Costa Rica, España y Paraguay- sitúan el delito de atentado contra los sistemas informáticos en el capítulo de los daños o ataques contra el patrimonio. Otras, lo ubican en un apartado afín a la seguridad informática -este es el caso de Chile, Ecuador, Panamá y República Dominicana-. Más adelante, al analizar la ubicación y su relación con el bien jurídico protegido, veremos a detalle la importancia de su discusión y reflexiva ubicación.

Argentina, Colombia y Ecuador han unido en un solo tipo penal los atentados contra los datos y sistemas informáticos. El resto de las legislaciones, emplean otra técnica: lo regula de forma independiente, es decir, como dos tipos penales individuales.

La denominación o *nomen iuris* es variada: *daño informático* (Colombia), *daños* (Argentina), *ataque a la integridad de los sistemas informáticos* (Ecuador y Chile), *sabotaje* (República Dominicana), *sabotaje informático* (Costa Rica) y *sabotaje de computadoras* (Paraguay).

El objeto sobre el cual recae la conducta ilícita también recoge diferentes denominaciones: *sistema informático*, *sistema de tratamiento de información*, *instalación de procesamiento*, *sistemas de tecnologías de información y comunicación*, *dispositivos electrónicos* e *infraestructuras tecnológicas*. Sería importante armonizar la legislación comparada, mientras tanto, debemos interpretar estos términos como sinónimos.

Solo Ecuador y España precisaron adecuadamente que la obstaculización del funcionamiento del sistema debe ser *grave*. Esta ausencia en el resto de las legislaciones estudiadas podría generar la sobre criminalización de las conductas.

Las legislaciones de Chile, España y Paraguay establecen expresamente que la obstaculización grave del funcionamiento del sistema informático debe producirse como consecuencia de una acción recaída sobre los datos informáticos, siguiendo la fórmula del Convenio de Budapest. Considero que esta construcción es adecuada y permite evitar o minimizar errores concursales.

7.5. LEGISLACIÓN NACIONAL

7.5.1. Antecedentes normativos

Dos proyectos de ley, presentados en 1999, fueron la base para la incorporación del delito de atentado contra los sistemas informáticos en nuestro Código Penal.

- **Proyecto de Ley N.° 5071/99-CR**, presentado el 18 de agosto de 1999 por el congresista Jorge Muñiz Ziches[696]. Esta propuesta normativa es la más cercana al tipo penal que finalmente se aprobó.
- **Proyecto de Ley N.° 5132/99-CR**, presentado el 31 de agosto de 1999 por la congresista Susana Díaz Díaz[697]. Esta propuesta recoge el término *maliciosamente* -que, como he dicho, no prosperó- y la construcción lingüística *sistema computacional* -que tampoco fue aprobado-. Sin embargo, debo destacar que, en este caso, se recomienda que el delito sea cometido empleando *medios computacionales*, característica de los ciberdelitos puros, pues en ellos se usan las TIC como instrumento y como objeto del ataque. De este modo, con claridad, se diferencia este ilícito del delito de daños.

De los diferentes tipos penales, este es el que más problemas tuvo en cuanto a su construcción, ya que los sistemas informáticos -elemento central del tipo penal- no eran reconocidos en esta época, sino a partir del 2001, con el Convenio de Budapest. De este modo, en el dictamen de la Comisión de Reforma de Códigos del 14 de junio de 2000 se precisó que "consideramos que la denominación de sistema informático no tiene una definición precisa dentro de la legislación nacional que involucre a las bases de datos, las redes, a los elementos informáticos integrantes del computador (*hardware* y software)". De este modo, para la Comisión la pluralidad de significados y acepciones no permitía uniformizar el tratamiento del compuesto *sistema informático*.

---

696 **Proyecto de Ley N.° 5071/99-CR, art. 209-B.-** El que indebidamente, [...] altere, dañe o destruya un [...] sistema o red será reprimido con pena privativa de la libertad no mayor de dos años.

697 **Proyecto de Ley N.° 5132/99-CR, art. 1.-** El que maliciosamente destruya o inutilice el soporte lógico de un sistema computacional, empleando medios computacionales, será reprimido con pena privativa de libertad no mayor a cuatro años.

En el debate del 21 de junio de 2000, se expuso y defendió la negativa a utilizar la construcción lingüística *sistema informático*:

> No es posible darle un contenido gramatical general, como decir "sistema informático", a situaciones o bienes que conjugan o integran este sistema, porque base de datos, redes, elementos informáticos, son utilizados de manera muy general por distintas entidades o personas. Por lo tanto, cuando se observa esta ley señalando que mejor utilicemos la denominación general "sistema informático", digo que esta definición es imprecisa dentro de nuestra legislación nacional y, sobre todo, de la legislación internacional. En consecuencia, tanto en la doctrina como en la legislación comparada no encontramos ninguna definición que diga, efectivamente, que "sistema informático" engloba a todo lo que es base de datos, redes o elementos informáticos. En tal sentido, el Congreso debe insistir en esta postura.

Finalmente, el delito fue incorporado como el artículo 207-B de nuestro Código Penal, permaneciendo vigente hasta el 2013, año en que se publicaría la LDI:

> **Art. 207-B CP.- Alteración, daño y destrucción de base de datos, sistema, red o programa de computadoras.** El que utiliza, ingresa o interfiere indebidamente [...] sistema, red [...] con el fin de alterarlos, dañarlos o destruirlos, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años y con setenta a noventa días multa.

En el 2001, el Convenio de Budapest uniformizaría el tratamiento de diversos términos, clasificándolos en dos: *datos informáticos* y *sistemas informáticos*. Si se hubiese aceptado la observación formulada por el Poder Ejecutivo, Perú hubiese sido líder regional en lo que a tipificación e innovación legal se refiere.

7.5.2. Génesis legislativa

Para comprender la redacción del delito de atentado contra la integridad de los sistemas informáticos que se encuentra vigente en nuestro país, es necesario remontarnos al proyecto de Ley N.º 34/2011. En él, el congresista Juan Carlos Eguren propuso la tipificación del delito de *sabotaje informático*,

recogiendo tanto la modalidad de atentado contra los datos como contra los sistemas informáticos. No obstante, el tipo penal que finalmente se aprobó tiene como origen el proyecto de Ley N.º 2520/2012, presentado por el Poder Ejecutivo, liderado por el presidente Ollanta Humala.

Lamentablemente, la única explicación o justificación en cuanto a la redacción se encuentra en la Exposición de Motivos. De hecho, el *nomen iuris* que, al igual que en el caso anterior, se propondrá modificar se origina en este segundo proyecto de ley, pues el congresista Eguren propuso denominarlo adecuadamente *sabotaje informático*.

Este delito se origina, al igual que en los casos previamente estudiados, en dos proyectos de ley:

- **Proyecto de Ley N.º 34/2011**, presentado el 11 de agosto de 2011 por el congresista Juan Carlos Neuenschwander.[698] La propuesta normativa (i) no incluye el medio por el cual se ocasiona la afectación de los sistemas informáticos; (ii) tampoco establece que la acción sea grave; (iii) propone sancionar cinco conductas: *destruir*, *dañar*, *modificar*, *alterar* e *inutilizar*; (iv) identifica el funcionamiento de los sistemas de información, de las TIC o sus componentes como el objeto material del delito.
- **Proyecto de Ley N.º 2520/2011**, presentado el 26 de julio de 2013 por el presidente de la República Ollanta Humala Tasso[699]. Esta fórmula es la que, finalmente, fue recogida en la LDI, debiendo destacar lo siguiente: (i) precisó que el medio comisivo son las TIC; (ii) recoge cuatro conductas típicas: *inutilizar*, *impedir el*

698 **Proyecto de Ley N.º 34/2011, art. 4. *Sabotaje informático.-*** El que destruya, dañe, modifique o realice cualquier acto que altere el normal funcionamiento o inutilice un sistema de información o una tecnología de información o cualquiera de los componentes que la conforman, será reprimido con pena privativa de libertad no menor de uno ni mayor de seis años.

699 **Proyecto de Ley N.º 2520/2011, art. 208-C. *Atentados a la integridad de sistemas informáticos.-*** El que, a través de las tecnologías de la información o de la comunicación, inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa.

acceso, *entorpecer* o *imposibilitar el funcionamiento*; (iii) establece que el sistema informático es el objeto de protección.

7.5.3. Evolución legislativa

Al igual que en el caso anterior, su modificación fue propuesta en dos proyectos de ley:

- **Proyecto de Ley N.° 2991/2013**, presentado el 25 de noviembre de 2013 por el congresista Juan Carlos Eguren Neuenschwander[700]. Este proyecto propuso (i) eliminar el medio comisivo (TIC) del tipo penal original e (ii) incluir los elementos *deliberada* e *ilegítimamente*.
- **Proyecto de Ley N.° 2999/2013**, presentado el 27 de noviembre de 2013 por el congresista Mauricio Mulder Bedoya[701]. Esta propuesta se acerca a la tipificación prevista en el Convenio de Budapest, en tanto (i) vincula el medio comisivo con la afectación de datos informáticos, (ii) propone incorporar los elementos *deliberada* e *ilegítimamente* en su construcción y (iii) simplifica o reduce la consecuencia ilícita a *afectar el funcionamiento de un sistema informático*.

7.5.4. Regulación actual

Desde su promulgación, el artículo 4 LDI ha sufrido una sola modificación suscitada en marzo del 2014. A continuación, veremos el texto original y lo contrastaremos con la fórmula vigente.

---

700 **Proyecto de Ley N.° 2991/2013, art. 4.** ***Atentado a la integridad de sistemas informáticos.***- El que deliberada e ilegítimamente inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa.

701 **Proyecto de Ley N.° 2999/2013, art. 4.** ***Atentado a la integridad de sistemas informáticos.***- El que de manera deliberada e ilegítima afecte el funcionamiento de un sistema informático mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa.

Art. 4 LDI (original)	Art. 4 LDI (actual)
Ley N.° 30096	Modificado por la Ley N.° 30171
El que, a través de las tecnologías de la información o de la comunicación, inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa.	El que deliberada e ilegítimamente inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa.

Cuadro 24. Regulación del delito de atentados contra la integridad de sistemas informáticos, 2013-2024. Elaboración propia.

La tipificación en el Convenio de Budapest y en la legislación local son dispares. Mientras que en el Convenio se utiliza el término *obstaculización* y se exige la *gravedad* como elemento objetivo del tipo, en Perú se opta por acudir a otras acciones: inutilizar, impedir el acceso, entorpecer o imposibilitar el funcionamiento o prestación de servicios de un sistema informático. La fórmula local genera problemas en la subsunción típica y en la interpretación de cada verbo rector.

De otro lado, mientras que en el Convenio se establece el medio que genera u origina la obstaculización grave del funcionamiento del sistema informático, Perú no hace alusión o referencia alguna.

	Convenio de Budapest	Convención de las Naciones Unidas contra la Ciberdelincuencia	Ley de Delitos Informáticos
	Ataques a la integridad del sistema (art. 5)	Interferencia con un sistema de tecnología de la información y las comunicaciones (art. 10)	Atentado a la integridad de sistemas informáticos (art. 4)
Obstaculización grave	X	X	-
Funcionamiento de un sistema informático	X	X	-
Inutiliza (total o parcial)	-	-	X
Impide el acceso	-	-	X
Entorpece el funcionamiento o prestación de servicios	-	-	X
Imposibilita el funcionamiento o prestación de servicios	-	-	X
Mediante	X	X	-
Introducción	X	X	-
Transmisión	X	X	-
Daño	X	X	-
Borrado	X	X	-
Deterioro	X	X	-
Alteración	X	X	-
Supresión	X	X	-

Cuadro 25. Comparación de los verbos rectores recogidos en el artículo 5 del Convenio de Budapest, en el artículo 10 de la Convención de las Naciones Unidas contra la Ciberdelincuencia y en el artículo 4 de la LDI. Elaboración propia.

La tipificación del delito de atentado contra la integridad de sistemas informáticos en la legislación penal peruana presenta la siguiente estructura:

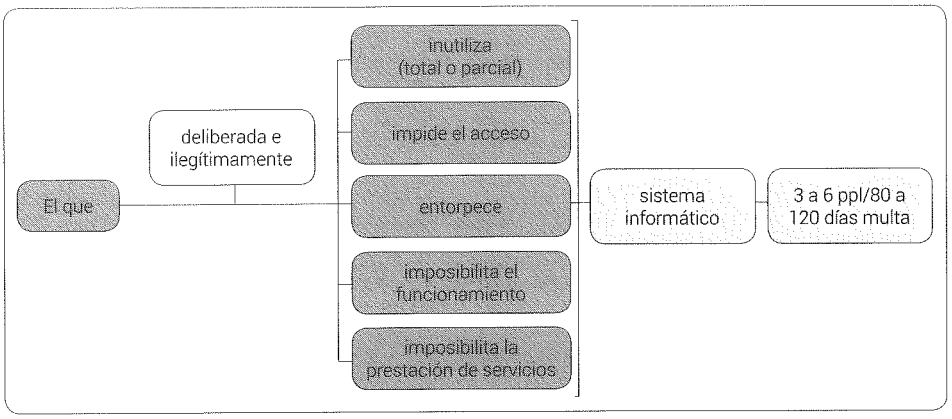


Diagrama 15. Estructura actual del delito de atentado contra la integridad de sistemas informáticos, en el sistema penal peruano. Elaboración propia.

7.6. EL BIEN JURÍDICO PENALMENTE PROTEGIDO

A nivel local, hay quien considera que el bien jurídico protegido es la intangibilidad informática[702], otros estiman que se protege la integridad informática, "entendiendo a ésta como el conjunto de datos y sistemas informáticos que se destruyen, inutilizan, dañan y/o modifican con la acción del ciberdelincuente"[703]. De manera más amplia, también se sostiene que protege la confidencialidad, integridad y disponibilidad -siguiendo el lineamiento pro-

702 Espinoza Calderón, *Delitos informáticos y nuevas modalidades delictivas*, cit., p. 80. En la misma línea: "Sin embargo, de la propia redacción del tipo penal se desprende que el bien jurídico protegido por el delito de atentado a la integridad de sistemas informáticos sería no solo la seguridad, sino también la intangibilidad del tráfico de información en la red" (Pérez López, *Delitos regulados en leyes penales especiales*, cit., p. 125).

703 Arévalo Minchola/Vega Aguilar, *Ciberdelitos. Análisis en el sistema penal*, cit., p. 288. En la misma línea: "En atención a lo expuesto, coincidimos que el bien jurídico es la integridad de los sistemas informáticos, por cuanto resulta necesario la protección de estos por cuanto han existido ataques dirigidos a servicios que brinda el estado en su funcionamiento debido a estos ataques, en tal sentido la protección del sistema en su conjunto resulta necesario" (Meneses Gonzáles/Meneses Ochoa, *La cibercriminalidad: Consideración criminológica, político-criminal, dogmática, procesal y cooperación internacional*, cit., p. 316).

puesto en el Convenio de Budapest-; pero se afirma que, al ser pluriofensivos, también se tutela la seguridad informática[704] -entendiendo este concepto como algo distinto a los tres elementos previamente descritos-.

Es importante advertir que se protege tanto la integridad como la disponibilidad de los sistemas informáticos. Lo expuesto en el Informe Explicativo da cuenta de ello: "El interés jurídico protegido es el interés de los operadores y los usuarios de los sistemas informáticos o de telecomunicaciones en su funcionamiento correcto".

Si entendemos que tanto una laptop como un sistema de telecomunicaciones, por ejemplo, son sistemas informáticos, entonces apreciaremos que la gravedad del daño ocasionado pudo ser un criterio empleado para diferenciar la intervención punitiva -por ejemplo, distinguir entre faltas y delitos, como indiqué anteriormente-. De hecho, tomando en consideración los ordenamientos analizados, solo España recoge el elemento *gravedad*-lo cual considero acertado, ya que, junto a Chile, es la legislación más cercana a la propuesta recogida en el Convenio de Budapest-.

En esta línea, a nivel comparado, las legislaciones de Colombia, Chile y España son las más cercanas a la propuesta legislativa recogida en el Convenio de Budapest.

Los sistemas informáticos pueden tener tanto componentes lógicos (*software*) como físicos o materiales (*hardware*). Este delito sanciona las conductas dirigidas contra el primer componente. Por esta razón, la destrucción física[705]

704 Jiménez Herrera, *Manual de derecho penal informático*, cit., p. 416.

705 La profesora Corcoy, a inicios de los noventa, con mucho detalle, explicaba las diferentes técnicas físicas utilizadas para dañar los sistemas informáticos: "Estas técnicas pueden consistir, por ejemplo, en: insertar cuchillas de hierro, clips o pequeñas piezas de aluminio dentro de la computadora para causar cortocircuitos tras un lapso de tiempo; echar residuos de café, soluciones salinas y agentes cáusticos de limpieza en la consola o en otros equipos; expandir humo de tabaco y spray del pelo u otros gases dentro del periférico -eje, una unidad de disco-; poner un recipiente con ácido clorhídrico enfrente de los conductos de inducción o succión del aire acondicionado o calentar partes sensibles de la computadora con cigarrillos encendidos; interferir en las fuentes de electricidad, conexiones o líneas de comunicación; meter ratones bajo un suelo elevado donde pueden roer los aislamientos de los sistemas de conexión o las propias conexiones; clavar una chincheta en los cables de conducción, lo que provoca fallos intermitentes..." (Corcoy Bidasolo, Mirentxu. "Protección penal del sabotaje

de una computadora, por ejemplo, arrojándola al suelo, no configura un ataque contra la integridad de los sistemas informáticos (art. 4 LDI), sino uno de daños (art. 205 CP)[706]. Ahora bien, las sanciones serán distintas pese a que, finalmente, se perdería la información contenida en el soporte físico: el ataque a un sistema informático recibe una pena que oscila entre tres y seis años de pena privativa de libertad, mientras que el delito de daños simples se castiga con una sanción no mayor a tres años. Una eventual reforma legislativa debería incidir también en la sanción que se impondrá para reprimir ambos tipos de conductas.

Delimitar el bien jurídico que se afecta específicamente con cada acto ilícito -propiedad o seguridad informática- es una labor realmente importante, no solo porque la sanción recibida será distinta, sino, además, porque en el caso de daños, el CP prevé una excusa absolutoria que no es aplicable a los delitos previstos en la LDI:

> **Art. 208 CP.-** No son reprimibles, sin perjuicio de la reparación civil, los [...] daños que se causen:
>
> 1. Los cónyuges, concubinos, ascendientes, descendientes y afines en línea recta.
> 2. El consorte viudo, respecto de los bienes de su difunto cónyuge, mientras no hayan pasado a poder de tercero.
> 3. Los hermanos y cuñados, si viviesen juntos.
>
> La excusa absolutoria no se aplica cuando el delito se comete en contextos de violencia contra las mujeres o integrantes del grupo familiar.

---

informático. Especial consideración de los delitos de daños". En: Mir Puig, Santiago [coord.]. *Delincuencia informática*. Barcelona: PPU, 1992, p. 148). Recomiendo la lectura del texto íntegramente, pues plantea los problemas sustantivos que se presentan en la tipificación de los delitos informáticos: criterios vinculados a la autoría y participación, el *iter criminis*, entre otros.

706 En la literatura española, hay quienes sostienen que nos encontramos frente a un problema concursal: "No hay acuerdo en la doctrina sobre como castigar una conducta sobre el soporte físico que causa al mismo tiempo la destrucción del elemento lógico. Algunos autores entienden que sería subsumible sin más en el art. 264 [González Reus, De la Mata Barranco, Hernández Díaz], mientras que otros opinan que debería castigarse tanto por el 263 como por el 264, en concurso ideal de delitos [Andrés Domínguez]. En todo caso, aquí no nos ocuparemos de la destrucción de *software* cometida únicamente a través de la destrucción física del *hardware*" (Gil Gil y Hernández Berlinches, *Cibercriminalidad,* cit., p. 215).

De este modo, si Jorge lanza por la ventana del quinto piso el ordenador de su hermana y el dispositivo se destruye, podríamos aplicar el artículo 208.1 CP como excusa absolutoria del delito de daños (art. 205 CP). Sin embargo, si Jorge dirige un ataque cibernético contra el sistema informático de su hermana, no podríamos aplicar dicha excusa, por cuanto estaríamos frente a un ataque contra la integridad del sistema (art. 4 LDI).

Ahora bien, existen casos sencillos que fácilmente podremos diferenciar: lanzar un celular contra el suelo, sumergir una computadora a una piscina, destruir un Apple Tv con un martillo, entre muchos otros[707]. Sin embargo, hay supuestos que caminan en la zona gris. Me refiero al uso del USB Killer[708]. Este dispositivo se conecta al puerto USB de un ordenador, recolecta la energía de las conexiones de alimentación hasta que alcanza los 220 voltios y, luego, se descarga muy rápidamente. Toda vez que este puerto soporta únicamente 5 voltios, en pocos segundos, el dispositivo se sobrecarga, afecta la placa base y, finalmente, el ordenador se daña.

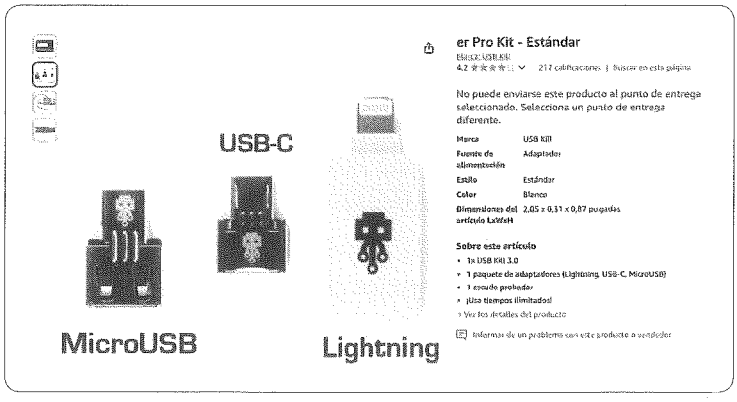


Imagen 23. El USB Killer es vendido en diversas plataformas, entre ellas, Amazon[709].

707 En la línea anteriormente descrita, se tiene: "Un delito de daños contra un sistema informático podría realizarse de varias maneras: la primera, mediante la destrucción física del continente o soporte material, es decir, del *hardware*, por ejemplo, destruyendo a martillazos el disco duro de un ordenador. Sin embargo, este tipo de daños se castigaría, como ya se ha dicho, a través del artículo 263 CP, que sería el destinado a proteger la seguridad física, o seguridad del *hardware*, y no del 264 o el 264 *bis*" (Gil Gil, "Daños informáticos", cit., p. 472).

708 Este dispositivo se diseñó alrededor del 2015 para probar sobretensiones y descargas electrostáticas en los componentes hardware de los ordenadores (Caballero/ Cilleros Serrano, *El libro del hacker. Edición 2022*, cit., p. 67.

709 Fecha de consulta: 28 de febrero de 2025. Disponible en: https://www.amazon.com/-/es/USB-Kill-Pro-Kit-Estándar/dp/B06ZZS7NFS

A continuación, analizaremos dos casos ocurridos en Estados Unidos y en España[710].

[Caso 90] El 14 de febrero de 2019, Vishwanath Akuthota, estudiante de 27 años, conectó un USB Killer en 66 computadoras y en numerosos monitores de The College of Saint Rose, ubicado en New York. La destrucción de 59 computadoras y 7 monitores generó una pérdida ascendente a 58 471 dólares americanos. Pocos meses después, aceptó su responsabilidad y fue condenado a 12 meses de prisión, seguido de un año de libertad supervisada[711].

[Caso 91] El Instituto de Biología y Genética Molecular es un centro mixto de investigación biomédica, ubicado en Valladolid, España.

El 13 de octubre de 2017, Juan adquirió un USB Killer, utilizando la cuenta prime de Amazon de su pareja. Así, pagó 89,56 euros por el modelo Pro kitA A-Estöjndar, el cual fue entregado cinco días después en la casa de la madre de su novia.

Juan utilizó el USB Killer entre el 19 y el 30 de octubre de 2017, afectando 20 computadoras, algunas de ellas eran de propiedad del Instituto de Biología y Genética Molecular, mientras que otras eran de becarios y docentes. Rápidamente, se elevó el problema a la empresa Hardtronic, la

710 La profesora Gil Gil recoge un caso muy interesante: "Una sentencia clasificadora de esta distinción es la que castigó por el 264 bis la destrucción de la placa base de varios ordenadores (lo que no es sino un elemento físico, parte del *hardware*) mediante una sobrecarga eléctrica producida por un USB Killer [...]. La sentencia recoge que no había daños en los discos duros y memorias, los datos que contenían los ordenadores no habían sido dañados y pudieron ser traspasados a ordenadores de sustitución, por lo que se absolvió del 264 CP. Hasta aquí tendríamos, por tanto, solo un delito de daños al *hardware*, reconducibles al art. 263. Sin embargo, la sentencia recoge que esas conductas "afectaron indirectamente a los objetos inmateriales de cada uno de los sistemas (*software*), entre ellos los drivers", provocando una obstaculización del sistema informático, lo que le permite la subsunción en el 264 *bis*" (Gil Gil, "Daños informáticos", cit., p. 497).

711 United States Attorney'S Office. *Former Student Sentenced For Destroying Computers at The College of St. Rose*, publicado el 13 de agosto de 2019. https://www.justice.gov/usao-ndny/pr/former-student-sentenced-destroying-computers-college-st-rose

cual brindaba mantenimiento a las máquinas del Instituto. El diagnóstico fue muy claro: fallo en las placas base, no atribuibles a USB dañados ni a problemas de voltaje de las instalaciones. De este modo, se concluyó que solo los USB Killer producen ese tipo de daños específicos y que la pérdida económica ascendía a 22130,89 euros.

El 8 de noviembre de 2017, después de realizar los actos descritos, Juan devolvió el USB Killer, extornándose los 89,56 euros pagados.

El Poder Judicial español concluyó que nos encontramos frente a actos que constituyen un delito continuado de daños a los sistemas informáticos, en concurso medial con la adquisición para su uso de programas informáticos maliciosos (abuso de mecanismos y dispositivos informáticos). Así, si bien la defensa argumentó que el dispositivo adquirido fue utilizado para conectarlo a una pecera y eliminar las bacterias, para el Tribunal esta hipótesis era débil, pues se acreditó que el ataque inició un día después de recibido el USB Killer y cesó cuando fue devuelto. Además, se valoró tanto la negativa de entregar su laptop como las opiniones técnicas de la policía y de quienes elaboraron los informes de mantenimiento[712].

7.7. TIPICIDAD OBJETIVA

7.7.1. Sujetos

Nos encontramos frente a un delito común, por lo que cualquier persona puede ser el **sujeto activo** de este delito. No se exige una condición o encargo especial.

Si bien hay posiciones que sostienen que "para acceder a un sistema informático se requiere de altos conocimientos sobre el tema [y] por tanto, el sujeto activo del delito debe tener esa cualidad"[713] o que este tipo de actos son

712 SAP VA 440/2020. Sentencia N.º 82/2020 del 8 de junio de 2020, emitida por la Audiencia Provincial de Valladolid, Sección N.º 2. Ponente: Juan Miguel Donis Carracedo.

713 Espinoza Calderón, *Delitos informáticos y nuevas modalidades delictivas*, cit., p. 83.

cometidos por *viruckers* o *crackers*[714], considero que no es correcto. Adoptar esta posición podría generar un sesgo de corroboración en el investigador al pensar que el ciberdelincuente necesariamente debe ostentar conocimientos especializados, cuando la redacción del tipo penal no lo exige. Sí, se presentarán ataques sofisticados en los que el delincuente contará con conocimientos técnicos altamente especializados, pero existirán otros en los que no ocurra esto.

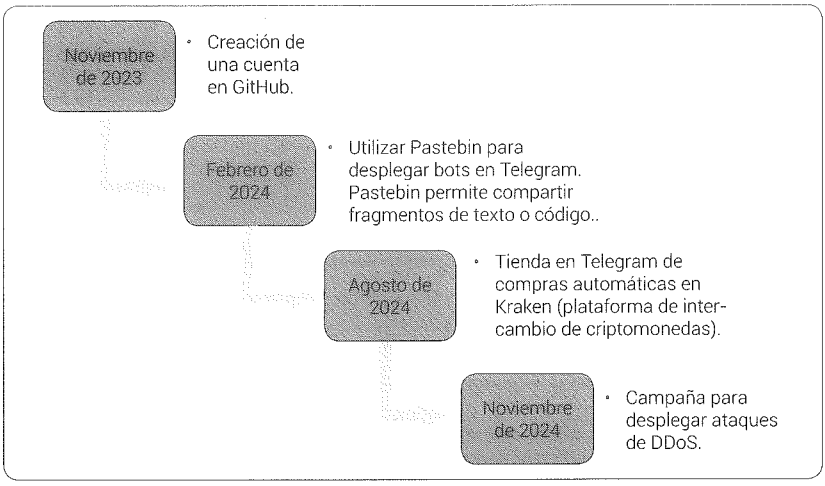
[Caso 92] A fines del 2024, investigadores de ciberseguridad identificaron un actor de amenazas que utilizaba el alias «Matrix». A cambio de un pago con criptomonedas, ofrecía ataques de denegación de servicio distribuido (DDoS) dirigidos contra dispositivos conectados a Internet (IoT). Dada las características de los servicios y las herramientas empleadas, se concluyó que nos encontrábamos frente a un *script kiddie,* un atacante que posee conocimientos básicos o muy limitados, pero que utiliza o compra herramientas existentes[715].

Este ejemplo grafica que, actualmente, los ciberdelincuentes no necesitan contar con conocimientos especializados, ya que, por ejemplo, podrían adquirir herramientas en el mercado negro con la finalidad de cometer sus ilícitas acciones.

El siguiente esquema explica los pasos que siguió el *script kiddie* «Matrix» en tan solo un año:

714 "Los agentes del delito, en la mayoría de estos casos, vienen a ser los *crackers* o los *viruckers*, como también podemos aceptar la posibilidad de que puedan ser otros sujetos que se encuentren dentro de la clasificación de los ciberdelincuentes. Se sostiene que estos sujetos son los ciberdelincuentes que cometen estos tipos de ilicitudes, ya que el tipo penal materia de análisis exige que se atente contra la integridad de los sistemas informáticos, vale decir, dañar, inutilizar o entorpecer el funcionamiento de los sistemas informáticos; todas estas consecuencias lo producen las actividades o conductas desviadas de los *crackers* o *viruckers*" (Jiménez Herrera, *Manual de derecho penal informático*, cit., p. 416).

715 Centro Nacional de Seguridad Digital. *Alerta integrada de seguridad digital N.º 275-2024*. Lima: 28 de noviembre de 2024, p. 4. https://www.gob.pe/institucion/pcm/informes-publicaciones/6247921-alerta-integrada-de-seguridad-digital-n-275-2024-cnsd



Esquema 2. Análisis de la actividad del actor de amenazas «Matrix» en GitHub, adaptado del gráfico inicialmente elaborado por Aqua Security[716].

En cuanto al **sujeto pasivo**, puede ser tanto una persona natural como jurídica; sin embargo, debe ser el titular del sistema informático vulnerado.

7.7.2. Acción típica

Es importante destacar que en el Perú no se ha recogido la forma o medio que origina el ataque al sistema informático y que fue sugerido en el Convenio de Budapest. El instrumento internacional precisa siete actos ilegales que podrían producir el ataque informático: introducción, transmisión, daño, borrado, deterioro, alteración y supresión de datos informáticos[717]. Nuestra legislación olvidó este extremo, lo que actualmente origina problemas en la aplicación de la norma en referencia. Una reforma legislativa, deberá incluir las modalidades que originan la afectación del sistema informático.

716 Dudinskikh, Karina. *La botnet Matrix desata ataques DDoS masivos explotando dispositivos IoT vulnerables*, en *UAD*, 27 de noviembre de 2024. https://unaaldia.hispasec.com/2024/11/la-botnet-matrix-desata-ataques-ddos-masivos-explotando-dispositivos-iot-vulnerables.html

717 El lector podrá observar que el artículo 5 del Convenio de Budapest incluye dos verbos que no fueron recogidos en el delito de ataques contra datos informáticos, previsto en el artículo 4 del Convenio. En este caso, los verbos cobran total sentido ya que su presencia puede afectar el funcionamiento del sistema. Los verbos en alusión son: *introducir* y *transmitir* datos informáticos.

Al analizar la redacción del tipo penal estudiado, fácilmente se advierte que la redacción de este delito no es la más adecuada. Como se ha indicado anteriormente, el proyecto de ley que lo originó no definió estos conceptos, sino que se limitó a resumirlos en los siguientes términos:

> Castiga a quien inutiliza, impide su acceso, entorpece o imposibilita el funcionamiento de sistemas informáticos o los servicios que estos prestan. Por ejemplo, a quienes saturan un sistema virtual de alguna entidad a través de accesos o requerimientos múltiples, impidiendo así su funcionamiento.

A continuación, propondré algunas definiciones que podrían servir de pautas de interpretación; sin embargo, como sugeriré más adelante, recomiendo modificar este delito para adecuarlo a la propuesta del Convenio de Budapest, es decir, emplear la fórmula *obstaculiza gravemente el funcionamiento del sistema*[718].

7.7.2.1. Inutilizar

La doctrina local define este término como "volver inservible el sistema informático"[719]; en la misma línea, se sostiene que esta modalidad se configura "cuando el daño ocasionado lo vuelve inútil para realizar las funciones por las cuales fue diseñado"[720].

Dicho esto, *inutilizar*, total o parcialmente, un sistema informático, quiere decir afectarlo de tal forma que pierde su utilidad, de forma permanente e irreversible. De todas las consecuencias posibles, es la más dañina.

Entre los *malwares* que inutilizan sistemas informáticos, encontramos los *wipers*. En nuestro país, el Comando Operacional de Ciberdefensa del Comando

---

718 Sobre este punto, el parágrafo 66 del Informe Explicativo indica: "El término "obstaculización" se refiere a las acciones que interfieren con el correcto funcionamiento del sistema informático. Dicha obstaculización debe efectuarse mediante la introducción, la transmisión, el daño, el borrado, la alteración o la supresión de datos informáticos".

719 Espinoza Calderón, *Delitos informáticos y nuevas modalidades delictivas*, cit., p. 83. En idéntico sentido, Arévalo Minchola/Vega Aguilar, *Ciberdelitos. Análisis en el sistema penal*, cit., p. 289.

720 Meneses Gonzáles/Meneses Ochoa, *La cibercriminalidad: Consideración criminológica, político-criminal, dogmática, procesal y cooperación internacional*, cit., p. 317.

Conjunto de las Fuerzas Armadas alertó en marzo del 2022 sobre la difusión de este tipo de *malware*:

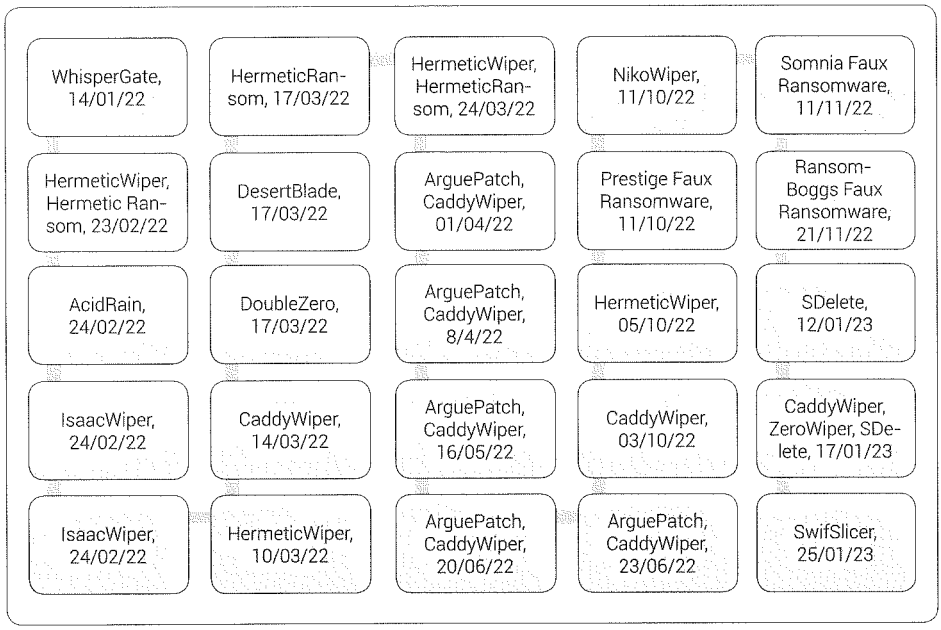
> En el caso de WhisperGate, se tiene conocimiento [de] que se trata de un *malware* diseñado para parecer un *ransomware*, pero cuya intención es realmente provocar daños irreparables. Se trata de uno de los llamados «wiper», es decir, un tipo de *malware* que busca borrar por completo el disco duro de la máquina afectada, deshaciéndose de toda la información y programas que hay en él. Lo que hace es sobrescribir por completo el MBR (es decir, el Registro de Arranque Principal) con una nota de rescate. Además, también intenta destruir la partición C:\ sobrescribiendo toda la información existente con datos aleatorios y sin sentido[721].

[Caso 93] El uso de los *wipers* con fines bélicos se masificó desde principios del 2022. Así, por ejemplo, diferentes cepas de *wipers* han sido empleados contra Ucrania: DoubleZero, WhisperKill, WhisperGate, HermeticWiper, IsaacWiper y CaddyWipper.

Los investigadores de ESET recopilaron cronológicamente los ataques de tipo *wiper* dirigidos contra Ucrania y que, en su mayoría, son atribuidos al grupo Sandworm. El objetivo, como se ha indicado, es inutilizar los sistemas informáticos objetivos. Veamos, a continuación, un recuento de ciberataques acontecidos en un año -no obstante, es importante indicar que no todos lograron sus objetivos, pues fueron identificados y evitados-[722].

721 Centro Nacional de Seguridad Digital. *Alerta integrada de seguridad digital N.º 65-2022*. Lima: 6 de marzo de 2022, p. 3. https://www.gob.pe/institucion/pcm/informes-publicaciones/2798506-alerta-integrada-de-seguridad-digital-n-065-2022-cnsd

722 ESET. "Un año de ataques de wiper apuntando a Ucrania", en *welivesecurity*, 27 de febrero de 2023. https://www.welivesecurity.com/la-es/2023/02/27/un-ano-ataques-wiper-apuntando-ucrania/



Esquema 3. Ciberataques dirigidos contra Ucrania, empleando *wipers* de enero de 2022 a enero de 2023. Elaboración propia.

[Caso 94] A mediados del 2010, la empresa de ciberseguridad VirusBlockAd informó sobre la existencia de un gusano creado para atacar centros industriales. Se cree que fue creado en Estados Unidos y que Israel habría colaborado para probar su efectividad, pues en el código del gusano se encontró la palabra *Myrthus*, que se interpreta como *Esther* -libro en el que se relata un complot persa para destruir Israel-.

El objetivo del *malware* Stuxnet era atacar y destruir máquinas centrifugadoras de centrales nucleares, las cuales son empleadas para la generación de energía y la construcción de armas nucleares.

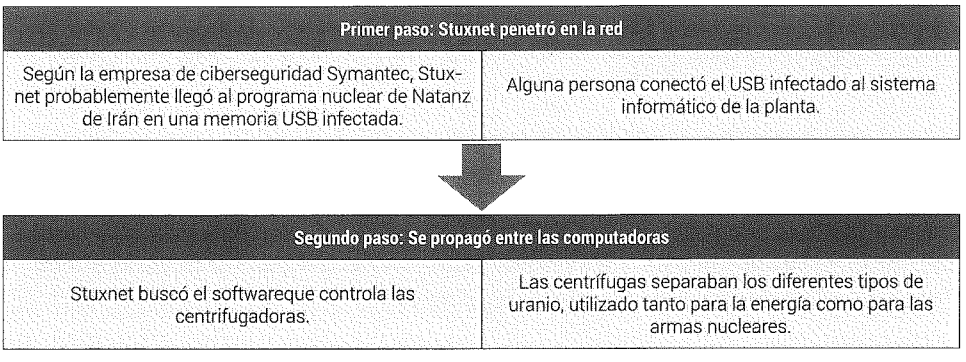
Si bien cierto sector calificó estos actos como ciberterrorismo[723], se discute si haber originado daños físicos a las centrifugas de la central nuclear puede

723 Caballero/Cilleros Serrano, *El libro del hacker. Edición 2022*, cit., pp. 119 y ss.

considerarse como un acto que implica un uso de la fuerza, prohibido por el Derecho Internacional[724]:

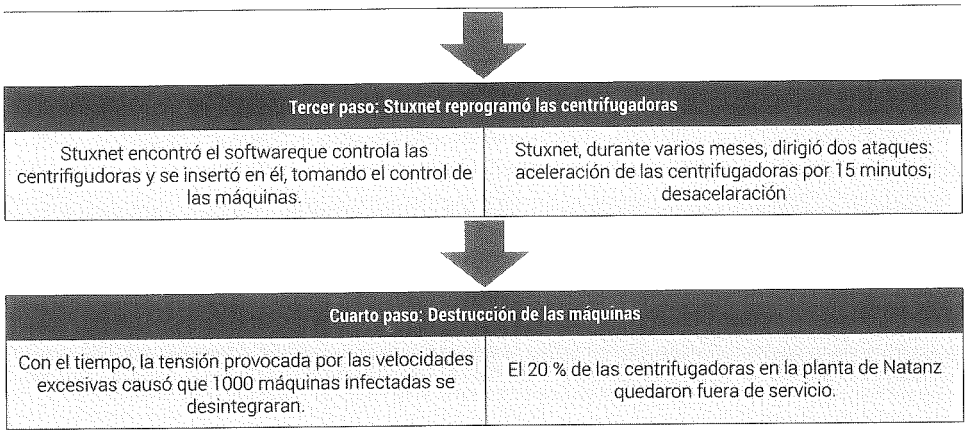
> Algunos ejemplos discutidos por el Grupo de Expertos y que muestran la falta de acuerdo son ilustrativos: en primer término, un ejemplo real, el Stuxnet, respecto del que unos miembros del Grupo de Expertos consideran que es un caso de ataque armado, a la luz del daño causado a las centrifugadoras iraníes, mientras que otros sostienen que solo es un uso de la fuerza prohibido, pero no un ataque armado. De donde se demostraría, para estos últimos, que el parámetro de la escala y efectos diferiría en los casos del ataque armado y del uso de la fuerza. La escala y efectos de los daños causados por el Stuxnet, siendo ese razonamiento -no expresado en los comentarios a la regla 71-, no serían tan severos como para que fuera calificado como un ataque armado. Y, como consecuencia, no cabría que Irán hubiese podido invocar legítima defensa para responder ante el Stuxnet[725].

Veamos, a continuación, cómo se realizó este ataque que generó preocupación y alarma por las consecuencias físicas que trajo:



724 Para comprender y profundizar el estudio de los nuevos escenarios bélicos y el uso de las TIC, recomiendo: Ambos, Kai. *Responsabilidad penal internacional en el ciberespacio*. Bogotá: Universidad Externado de Colombia, 2014.

725 Pérez-Prat Durbán, Luis. "Los ciberataques y el uso de la fuerza en las relaciones internacionales". En: Millán Moro, Lucía (dir.). *Ciberataques y ciberseguridad en la escena internacional*. Navarra: Thomson Reuters / Aranzadi, 2019, p. 45.



Esquema 4. Pasos del ciberataque Stuxnet que dañó 1000 centrifugadoras de una central nuclear iraní[726].

En este caso, se advierte la destrucción del soporte físico como parte del ataque dirigido contra el sistema informático, sin embargo, esto no es indispensable para que esta modalidad se configure. De hecho, en la mayoría de las ocasiones, será el soporte lógico del sistema el que resulte inutilizado.

7.7.2.2. Impedir (el acceso)

Si bien Chile recoge el verbo impedir, lo vincula con el funcionamiento adecuado del sistema y no con el acceso a este. Así, el referido ordenamiento sanciona a quien "obstaculice o impida el normal funcionamiento, total o parcial, de un sistema informático"[727].

A nivel local, cierto sector lo define como la acción de "no permitir que los propietarios del sistema informático puedan acceder"[728], otro lo entiende

726 Los pasos y las definiciones han sido adaptados de: "El virus que tomó control de mil máquinas y les ordenó autodestruirse", en *BBC Mundo*, 11 de octubre de 2015. https://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet

727 En España, se recoge el siguiente caso: "Otro ejemplo en nuestra jurisprudencia de obstaculización del sistema mediante esta modalidad es la alteración de las cuentas de los usuarios (datos del sistema) abusando, de forma no autorizada, de los privilegios de administrador, provocando así el bloqueo del servidor del Ayuntamiento y que no pudiera acceder al mismo ningún usuario" (Gil Gil, "Daños informáticos", cit., p. 497).

728 Espinoza Calderón, *Delitos informáticos y nuevas modalidades delictivas*, cit., p. 83.

como "bloquear o restringir el acceso a un determinado sistema informático"[729], sosteniendo que, de esta forma, se cierran los espacios de impunidad posibles.

Sostengo que *impedir el acceso* al sistema informático debe entenderse como la imposibilidad de que el usuario autorizado ingrese y lo utilice. Esta modalidad afecta la disponibilidad del sistema, ya que impide por completo su ingreso o acceso.

[Caso 95] Con fines pedagógicos, esta modalidad puede ilustrarse con el siguiente ejemplo: un ataque dirigido al sistema informático de una entidad bancaria que impide a los usuarios acceder a la información de sus cuentas a través de aplicaciones móviles o plataformas web[730]. La normativa peruana no exige que sea la propia entidad la afectada directamente en su acceso al sistema, sino que también contempla válidamente la afectación a sus usuarios.

En el 2024, el banco Santander Chile sufrió un ataque de denegación de servicios, lo que originó que sus usuarios no pudieran acceder a sus plataformas. La entidad bancaria subió una declaración pública a su página web. En ella reconoce el ataque y los daños causados, pero asegura que la información de sus clientes no se vio expuesta:

> Santander Chile tuvo una incidencia de denegación de servicios, produciéndose una sobrecarga en el acceso a los canales de atención como el sitio web, App Santander y Office Banking. Frente a esta situación, el banco aplicó de forma inmediata sus protocolos y medidas para gestionar el incidente, reestablecer el servicio y proteger a nuestros clientes.
>
> Cabe destacar que este tipo de casos no implica una vulneración a los sistemas del Banco, por lo que nuestros clientes pueden operar con seguridad.
>
> Lamentamos los inconvenientes que esta situación pudo haber generado por la intermitencia de los canales digitales[731].

729 Arévalo Minchola/Vega Aguilar, *Ciberdelitos. Análisis en el sistema penal*, cit., p. 289.

730 Meneses Gonzáles/Meneses Ochoa, *La cibercriminalidad: Consideración criminológica, político-criminal, dogmática, procesal y cooperación internacional*, cit., p. 317.

731 *Declaración pública de Santander Chile,* Santiago de Chile, 23 de octubre de 2024. https://saladecomunicacion.santander.cl/noticias/institucional/detalles/declaracion-publica

[Caso 96] Algunos tipos de *ransomware* cifran el sistema utilizando el mismo método de encriptación del disco duro del usuario. Como resultado, al encender el ordenador, la única pantalla que aparece indica los pasos para pagar un *rescate* a cambio de recuperar el acceso al sistema. Las consecuencias varían según el tipo de dispositivo afectado: puede tratarse tanto del ordenador personal de un estudiante como del servidor central de una infraestructura de comunicaciones[732].

En nuestros hogares, es cada vez más frecuente contar con un *smart* TV. Lamentablemente, en el 2024, se identificaron diversos *malwares* que los afectan, incluso ataques de *ransomware* que impiden que el usuario acceda a su televisión si no paga un pequeño rescate[733].

7.7.2.3. Entorpecer

A nivel comparado, Costa Rica utiliza una fórmula similar a la recogida en el ordenamiento peruano. Veamos: "Si como resultado de las conductas indicadas se entorpece [...] el funcionamiento de un programa de cómputo, una base de datos o un sistema informático [...]".

En la doctrina local, para Espinoza Calderón, es "dificultar el acceso al sistema"[734]. En tanto, para Vega Aguilar y Arévalo Minchola, "esta modalidad se encuentra relacionada con la siguiente (imposibilitar el funcionamiento) y parten del hecho de reprimir las conductas que obstaculicen no solo el acceso, sino el trabajo de los sistemas informáticos"[735]. Meneses Gonzáles y Meneses Ochoa critican la técnica legislativa al considerar que "deviene en redundante

732 Entre los tipos, tenemos: (1) *Ransomware* de cifrado, (2) *ransomware* de bloqueo de pantalla, (3) *ransomware* de cifrado de arranque, (4) *ransomware* híbrido, (5) *ransomware* de filtración de datos, (6) *ransomware* de doble extorsión y (7) *ransomware* como servicio (Vargas Carpio, Mónica Rocío. "Ataques cibernéticos de tipo *ransomware*". En: Espinoza Calderón, Víctor Raúl [coord.]. *Cibercriminalidad y delitos informáticos*. Lima: Instituto Pacífico, 2023, pp. 662 y s.).

733 "Cuida tu Smart TV, este es el virus que puede dañarlo y espiarte", en *Infobae*, 6 de abril de 2024. https://www.infobae.com/tecno/2024/04/06/cuida-tu-smart-tv-este-es-el-virus-que-puede-danarlo-y-espiarte/

734 Espinoza Calderón, *Delitos informáticos y nuevas modalidades delictivas*, cit., p. 83.

735 Arévalo Minchola/Vega Aguilar, *Ciberdelitos. Análisis en el sistema penal*, cit., p. 292.

en colocar acciones repetidas que solamente generan confusión y problemas al momento de su aplicación. Sobre esta acción podemos resumirla en la acción de afectar el correcto funcionamiento del sistema informático"[736].

En esta obra, sostengo que *entorpecer* el funcionamiento del sistema informático quiere decir ralentizarlo, retardarlo o dificultar su empleo. Así, el usuario no pierde el acceso, pero ve mermada su experiencia de uso.

[Caso 97] Minar criptomonedas es una actividad costosa: requiere alto consumo de energía eléctrica, contar con múltiples CPU que tengan *hardware* y *software* los suficientemente potentes para ejecutar continuamente el proceso de minado. En algún momento, los ciberdelincuentes se dieron cuenta de que, en vez de adquirir computadoras para este propósito, podían infectar decenas, cientos o miles de máquinas de otros usuarios para que realicen esta labor. De este modo, el dispositivo seguirá funcionando, pero el usuario legítimo advertirá que *corre lentamente*, ya que, sin saberlo, está ejecutando programas para la minería de criptomonedas[737].

En el 2021, se difundió un *malware* del tipo *criptojacking* denominado Pro-Ocean. Este *software* malicioso explotaba las vulnerabilidades conocidas para apuntar a aplicaciones en la nube y, de este modo, minimizar cualquier uso del CPU y utilizar al máximo su capacidad para minar criptomonedas desde el dispositivo infectado, sin que la víctima lo supiera.

Pro-Ocean contenía cuatro módulos que se desplegaban durante la ejecución: ocultación, minería, infección y vigilancia[738].

736 Meneses Gonzáles/Meneses Ochoa, *La cibercriminalidad: Consideración criminológica, político-criminal, dogmática, procesal y cooperación internacional*, cit., p. 318.

737 "El *cryptojacking* es el uso no autorizado de la potencia de un sistema ajeno para minar criptomonedas" (Caballero/Cilleros Serrano, *El libro del hacker. Edición 2022*, cit., p. 96).

738 Centro Nacional de Seguridad Digital. *Alerta integrada de seguridad digital N.º 23-2021*. Lima: 1 de febrero de 2021, p. 3. https://www.gob.pe/institucion/pcm/informes-publicaciones/1625620-alerta-integrada-de-seguridad-digital-n-023-2021-pecert. También, Sasson, Aviv. *Pro-Ocean: Rocke Group's New Cryptojacking Malware* del 28 de enero de 2021. https://unit42.paloaltonetworks.com/pro-ocean-rocke-groups-new-cryptojacking-malware/

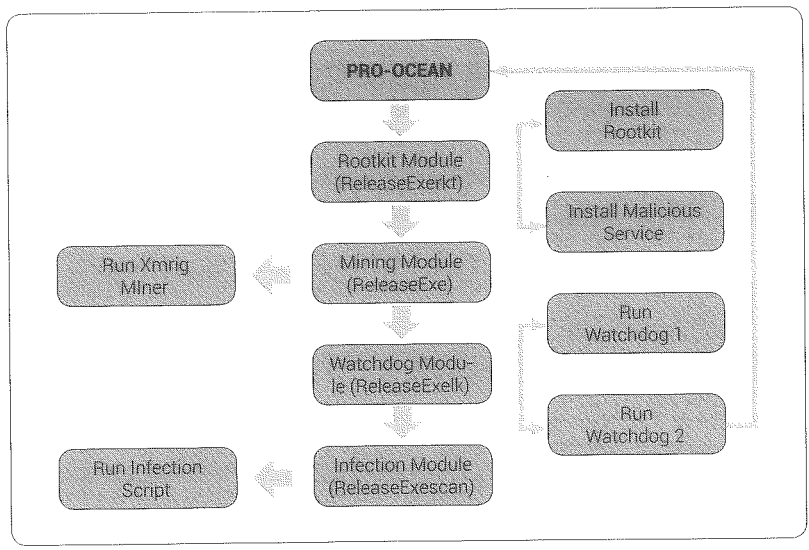


Diagrama 16. Funcionamiento del *malware* Pro-Ocean.

7.7.2.4. Imposibilitar

A nivel local, se entiende que, a través de esta conducta, se obstaculiza el funcionamiento de un sistema informático o la prestación de un servicio brindado mediante este[739]. En la literatura también se acuña el siguiente concepto: "Esta modalidad típica consiste en incapacitar o quitar la posibilidad de funcionamiento del sistema informático. Igual que en el verbo típico precedente, esta modalidad no se encuentra establecida en el Convenio de Budapest; sin embargo, de su propio tenor se puede colegir que todo acto de imposibilidad de funcionamiento implica un acto lesivo y grave de obstaculización de los sistemas informáticos"[740].

En este caso, no se impide el acceso al sistema informático, sino que afecta su utilidad de forma temporal o de manera reversible. Como el lector podrá notar, la diferencia entre *imposibilitar* e *inutilizar* radica en la permanencia o temporalidad de la afectación.

739 Espinoza Calderón, *Delitos informáticos y nuevas modalidades delictivas*, cit., p. 83.

740 Arévalo Minchola/Vega Aguilar, *Ciberdelitos. Análisis en el sistema penal*, cit., p. 292.

[Caso 98] Actualmente, las empresas y corporaciones suelen tercerizar cierto tipo de servicios. Por ejemplo, el registro de ingreso y salida de sus empleados, los sueldos que deben abonarse o las vacaciones que deben gozar. En noviembre de 2024, la empresa Blue Yonder fue víctima de un ataque de *ransomware,* impidiendo que prestara sus servicios a empresas como Starbucks o a la cadena de supermercados británicos Morrison y Sainsbury's[741].

De este modo, Starbucks, por ejemplo, no podía realizar el seguimiento de las horas trabajadas y los pagos a efectuar a sus empleados. Tuvieron que regresar al lápiz y papel durante los días que los servicios prestados por Blue Yonder fueron impedidos por el ciberataque en referencia.

A modo de resumen, la definición propuesta para los verbos rectores de este delito es la siguiente:

Verbo	Definición propuesta
Inutilizar	Evitar permanentemente el funcionamiento del sistema.
Imposibilitar	Evitar temporalmente el funcionamiento del sistema informático o la prestación de sus servicios.
Impedir	Evitar el acceso al sistema informático.
Entorpecer	Ralentizar, retardar o dificultar el empleo del sistema informático.

Cuadro 26. Resumen de definiciones propuestas de los verbos que integran delito de atentado a la integridad de sistemas informáticos. Elaboración propia.

7.7.3. Objeto del delito

Pérez López sostiene que el objeto material del delito es el sistema informático, precisando, además, que "se afectarían los datos informáticos"[742]. Coincido con esta posición, este artículo sanciona las acciones cometidas contra

741 Centro Nacional de Seguridad Digital. *Alerta integrada de seguridad digital N.º 273-2024.* Lima: 26 de noviembre de 2024, p. 4. https://www.gob.pe/institucion/pcm/informes-publicaciones/6232419-alerta-integrada-de-seguridad-digital-n-273-2024-cnsd. También: Entrepeneur en español. *Ataque de ransomware afecta operaciones de Starbucks y grandes supermercados,* publicado el 26 de noviembre de 2025. https://www.entrepreneur.com/es/noticias/ataque-de-ransomware-afecta-operaciones-de-starbucks-y/483508

742 Pérez López, *Delitos regulados en leyes penales especiales,* cit., p. 130.

los sistemas informáticos, específicamente contra su funcionamiento o contra la prestación de servicios.

Es importante señalar que el Convenio de Budapest contempla únicamente el *funcionamiento* de los sistemas informáticos como objeto del delito. No obstante, el legislador peruano optó por incluir también la *prestación de servicios*, presumiblemente con el fin de abarcar un espectro más amplio de conductas, aunque esta inclusión resulta, en rigor, innecesaria.

7.7.3.1. Funcionamiento

Considero que el elemento *funcionamiento* debe entenderse como la capacidad interna de ejecutar procesos, transmitir información o realizar las funciones para las que fue diseñado el sistema.

Sobre la afectación al sistema informático, la fórmula recogida en España es la más cercana al Convenio de Budapest: "Será castigado con la pena de prisión de seis meses a tres años el que, sin estar autorizado y de manera grave, obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno [...]".

La catedrática Gil Gil recoge casuística de la jurisprudencia española para explicar la diferencia de un ataque a los datos de uno a los sistemas informáticos. Considero que el caso seleccionado y su reflexión es adecuada.

> **[Caso 99]** "Más dudosa, en cambio, es la calificación que por este tipo se realizó de la sustitución de las tarjetas de memoria por otras que contenían archivos diferentes a los necesarios para la finalidad que se pretendía (proyectar una exposición), o mal configurados. En este caso, en mi opinión, el tribunal aplicó la idea de 'obstaculización del sistema' de manera excesivamente amplia, confundiendo el daño al propio sistema con la frustración de los fines o servicios para los que su legítimo propietario había previsto la utilización del sistema. Si estos últimos no se cumplieron (a falta de suficientes detalles técnicos en la sentencia), parece que no fue porque el sistema informático no funcionara, sino porque la información que debía contener fue sustituida por otra. En mi opinión, este supuesto debió llevarse por el 264"[743].

743 Gil Gil, "Daños informáticos", cit., p. 497.

7.7.3.2. Prestación de servicios

Este elemento no está incluido en el Convenio sobre la Ciberdelincuencia. Soy de la opinión que resulta innecesario incluir la expresión *prestación de servicios,* en tanto, es la consecuencia de la obstaculización del funcionamiento del sistema. Sin embargo, en tanto nuestra legislación contempla esta figura, se ha de identificar alguna definición que evite contradicciones.

Considero que por *prestación de servicios* debe entenderse la oferta o puesta a disposición de terceros de los servicios, en la forma como fue diseñado el sistema informático.

[Caso 100] Hoy en día, los sistemas informáticos están relacionados a la prestación de servicios básicos como el agua o la energía eléctrica. El 23 de diciembre de 2015, la mitad de los hogares de la región ucraniana Ivano-Frankivsk se quedó sin electricidad. Los ciberdelincuentes utilizaron el *malware* BlackEnergy para instalar un componente KillDisk. Así, borraron los archivos del sistema para que los equipos no puedan arrancar.

Pese a que en Ucrania no se celebra la Navidad, los atacantes eligieron estas festividades para distribuir correos electrónicos maliciosos en el que suplantaban la identidad del remitente y, de este modo, persuadir a las víctimas para que ejecuten el macro de los documentos adjuntos. Diversos usuarios de empresas eléctricas ucranianas cayeron en el ataque de ingeniería social. El resultado: apagones y fallas eléctricas en una región de un millón y medio de habitantes[744].

7.8. TIPICIDAD SUBJETIVA

Al igual que en análisis previos, esta conducta exige tanto una actuación dolosa como deliberada. Es decir, el sujeto activo conoce que está llevando a cabo alguno de los verbos rectores aquí descritos. Incorporar el término *deliberadamente* permite afirmar que el dolo eventual no es punible, por lo que se recomienda modificar este extremo del tipo penal -más aún cuando ninguna otra

744 Lipvsky, Robert. "El troyano BlackEnergy ataca una plata de energía eléctrica en Ucrania", en *welivesecurity*, 5 de enero de 2016. https://www.welivesecurity.com/la-es/2016/01/05/troyano-blackenergy-ataca-planta-energia-electrica-ucrania/

legislación comparada analizada hace uso de esta expresión-. Para Oré Sosa, "más que acreditar un *animus nocendi* o intención de dañar, lo que se debe imputar es el conocimiento de la potencialidad lesiva de la conducta, esto es, la posibilidad de que se produzca el resultado de inutilización o entorpecimiento"[745].

Algunos autores peruanos consideran adecuada esta precisión: "La introducción del término *deliberado* ha venido a complementar el aspecto subjetivo, dotando con claridad la exigencia de presentación de dolo directo para la comisión del referido delito". Discrepo de esta posición, pues genera problemas de interpretación, prueba y un vacío punitivo que, precisamente, se reclama.

7.9. LAS SITUACIONES DE JUSTIFICACIÓN EN EL DELITO DE ATENTADO A LA INTEGRIDAD DE SISTEMAS INFORMÁTICOS

La conducta desplegada debe ser ilícita, es decir, contraria al ordenamiento y no debe existir una causa de justificación. El Informe Explicativo lo ha graficado en el parágrafo 68 de la siguiente manera: "Las actividades comunes inherentes al diseño de las redes, o las prácticas comerciales y de operación comunes, se efectúan de manera legítima. Las mismas incluyen, por ej., la verificación de la seguridad de un sistema informático, o su protección, autorizada por su propietario o por el operador, o la reconfiguración del sistema operativo de un ordenador que tiene lugar cuando el operador de un sistema instala un nuevo *software* que inhabilita programas similares previamente instalados. Por lo tanto, dicha conducta no constituye un delito conforme a este artículo, incluso si causa una obstaculización seria".

Como he indicado anteriormente, al encontrarse regulado en el Código Penal, la LDI no necesita que se reitere que la conducta debe ser ilícita, por lo que una eventual modificación debería suprimir esta expresión. Este punto se ve reforzado con el análisis de la legislación comparada, ya que el resto de los países, como se ha dicho, no han incluido los elementos *deliberada* e *ilegítimamente* en sus respectivas redacciones.

En efecto, pensemos en el siguiente escenario: los sistemas informáticos de una empresa están siendo atacados. Ya que el agraviado necesita repeler el ataque, contrata un ciberdelincuente para que neutralice al actor de amenaza.

745 Oré Sosa, *Delictum. Apuntes de derecho penal*, cit., p. 196.

¿Es legítimo reprimir penalmente a quien necesita repeler un ciberataque? El profesor Jesús María Silva Sánchez sostiene que no -posición que comparto-:

> La doctrina de los procedimientos institucionalizados constituye un mecanismo a favor de la resolución pacífica de los conflictos, atribuida al Estado. Sin embargo, en aquellos casos en los que el procedimiento establecido no conlleva una solución efectiva del problema, sostener que el agredido que reacciona de modo defensivo realiza una lesión antijurídica del bien del agresor resulta excesivo. No en vano, la propia existencia de una agresión antijurídica pone de relieve que el Estado no ha conseguido la protección preventiva de los bienes del agredido. En definitiva, la legítima defensa del patrimonio mediante reacciones que no afecten a bienes intrínsecos del agresor debe ser posible. La única excepción a ello es la existencia de un procedimiento legal que garantice realmente la protección del patrimonio amenazado, de forma rápida y razonablemente segura. Solo en tal caso, además, puede afirmarse que los bienes no se encuentran en riesgo de deterioro o pérdida inminente. Por lo demás, la existencia de un procedimiento eficaz -aunque se oponga a la apreciación de una legítima defensa justificante-, en general no puede desvirtuar la estimación de una defensa necesaria eximente de pena. En fin, cuando la agresión es extraterritorial, la existencia de procedimientos institucionalizados en el territorio no parece ofrecer una base suficiente para la limitación de la legítima defensa. Así pues, el afectado puede repeler lícitamente la conducta del agresor externo mediante una reacción contra los bienes de este. Un ejemplo relevante es el de los ciberataques que amenazan con la destrucción de datos o directamente lesionan la propiedad intelectual del agredido. Por tanto, en estos casos, **la defensa mediante la contratación de un pirata informático para destruir la fuente de la que proceden los ciberataques es legítima** [El resaltado es mío][746].

746 Silva Sánchez, *Derecho penal. Parte general*, cit., p. 1433.

7.10. CONSUMACIÓN

La doctrina nacional es pacífica al aceptar que estamos frente a un delito de resultado y que, en consecuencia, es posible sancionar la tentativa[747]. En efecto, no basta con que el sujeto activo realice la conducta ilegal, sino que, además, se debe lograr el resultado: impedir el acceso, imposibilitar su funcionamiento o prestación de sus servicios[748].

Así, por ejemplo, siguiendo a Miró Llinares, se tienen casos de envío de *malware* destructivo que, sin embargo, es detectado a tiempo por las especiales barreras de seguridad informática como antivirus o *firewalls*[749].

Desde el ámbito probatorio, es importante recordar que se debe acreditar la relación de causalidad que debe conectar la acción típica y el resultado lesivo. Dicho de otro modo, debe corroborarse que el daño que sufrió el sistema informático se conecta a la acción reputada al agente. En Argentina, por ejemplo, se recuerda el caso Fibertel, en el que se acusó a un exempleado de emplear un programa malicioso y, de este modo, afectar el funcionamiento y la integridad del sistema de tratamiento y almacenamiento de datos ofrecidos a terceros. Sin embargo, en el juicio, la relación causal no se acreditó, absolviéndose al acusado[750].

El atentado contra la integridad o disponibilidad de un sistema informático puede adoptar diferentes formas, pasos y procedimientos. Una de las diferentes modalidades podría emplear la siguiente cadena de ataque:

747 Arévalo Minchola/Vega Aguilar, *Ciberdelitos. Análisis en el sistema penal*, cit., p. 295. En el mismo sentido, Jiménez Herrera, *Manual de derecho penal informático*, cit., p. 417.

748 Pérez López, *Delitos regulados en leyes penales especiales*, cit., p. 131.

749 Oré Sosa, *Delictum. Apuntes de derecho penal*, cit., p. 196.

750 Aboso, *Derecho penal cibernético: La cibercriminalidad y el derecho penal en la moderna sociedad de la información y la tecnología de la comunicación*, cit., p. 363.

1. *Footprinting* o reconocimiento

- Consiste en identificar el entorno que será atacado: arquitectura de la red, hosts, servidores, móviles, máquinas virtualizadas, tecnologías que incluyen, etc.
- Existen dos reconocimientos: pasivo y activo.

2. *Fingerprinting* o escaneo y enumeración

- Consiste en recoger información de manera activa mediante herramientas y técnicas concretas para llegar a conocer a fondo el objetivo del ataque.
- Ejemplo: escaneo de direcciones de IP de la red, utilizar un escaneo de vulnerabilidades.

3. Intrusión y toma de control

- Los ataques pueden ser simples, como acceder a un punto de acceso wifi no securizado o tan complejo como explotar un *zero-day*, a través de herramientas metaexploit, lanzar un *SQL Injection* (XSS) a través de una web o escribir y lanzar un ataque de *buffer overflow* a un sistema para que quede inaccesible.
- Una vez escrito y probado el *malware*, se ejecuta y, si el ataque tiene éxito, continúa.

4. Mantener el acceso y robo de información

- El atacante necesita comprobar que puede volver a entrar al sistema, razón por la cual identifica puertas traseras (*backdoors*) usando troyanos u otro tipo de *malware*.
- Se trata de escalar privilegios para hacerse del dominio del sistema desde un usuario a nivel rooto de administrador. Caso contrario, no podrá instalar *malware* para futuras intrusiones.

5. Cubrir el ataque

- Se trata de eliminar todo tipo de huella frente a un posible análisis forense.
- En este camino, se eliminarán ficheros, logso se ocultarán con atributos de ocultación de ficheros y directorios.

Esquema 5. Pasos y etapas de una cadena de ataque contra un sistema informático[751].

Insisto en señalar que esta es una cadena de ataque. Se pueden identificar otras tantas, con más o menos pasos. Mi intención es ejemplificar el procedimiento, ya que no todos los pasos serán penalmente relevantes. Así, por ejemplo, si únicamente he identificado la arquitectura de red, ni siquiera podría considerarse que he dado inicio al ataque. Podría considerarse un acto preparatorio y, en consecuencia, no ser punible. Lo mismo sucederá con la fase denominada *cubrir el ataque*. En esta etapa, el delincuente ya atacó el sistema informático y logró su objetivo, pero está tratando de borrar sus huellas digitales. Considero que estos actos son posteriores a la consumación, pero podrían configurar otro delito, por ejemplo, daños a datos informáticos (al eliminar determinados datos con la finalidad de no ser descubierto).

7.11. CONCURSOS

Algunos autores consideran que existe una relación secuencial entre el delito de acceso ilícito y el atentado a sistemas informáticos:

751 Los pasos y las definiciones han sido tomados y adaptados de: Caballero/Cilleros Serrano, *El libro del hacker. Edición 2022*, cit., pp. 103-106.

> Para analizar este delito debemos partir de que los ciberdelitos puros que son los que forman parte de este segundo capítulo de la Ley N.º 30096 constituyen una secuencia de conductas que inicia con el acceso a un determinado sistema informático; y, por ende, todo acto de alteración, daño, y/o modificación de un sistema informático va a partir de un acceso ilícito como primer acto [...]. Si queremos realizar una enumeración concreta de esta secuencia de conductas, diríamos que se inicia con un acceso ilícito y luego puede producir resultados, ya sea en un dato informático (sería constitutivo del delito de atentado contra datos informáticos) o en un sistema informático (sería constitutivo del delito que analizamos actualmente).
>
> En la secuencia cibercriminal, el delito que analizamos resulta ser un segundo momento, posterior al acceso ilícito. De ahí que toda conducta de alteración de un sistema informático requiera que previamente haya existido un acceso ilícito a un determinado sistema [...][752]

En efecto, en algunos casos, los ciberdelincuentes accederán ilegalmente a los sistemas informáticos antes de atentar contra su integridad; sin embargo, ambos delitos no son necesariamente secuenciales. Así, existen sabotajes informáticos en los que no se producen accesos ilícitos previamente. Por esta razón, es importante identificar el comportamiento del agente y la modalidad empleada.

En la legislación penal peruana existe un concurso de leyes aparente entre el delito de daños (art. 200 CP) y el delito de atentado a la integridad de los sistemas informáticos (art. 4 LDI). En aplicación del principio de especialidad[753], este último desplaza al primero.

A continuación, analicemos algunas situaciones problemáticas.

Si un ciberdelincuente dirige un ataque de *ransomware* contra una empresa y encripta todos sus sistemas informáticos, estaremos frente a un *concurso*

752 Arévalo Minchola/Vega Aguilar, *Ciberdelitos. Análisis en el sistema penal*, cit., p. 286.

753 "El principio de especialidad es posiblemente el más extendido de los principios que se utiliza para determinar cuál es la ley penal aplicable en un concurso de leyes. Este principio establece que debe aplicarse el tipo penal que regula más específicamente la integridad del hecho concretamente realizado: *lex specialis derogat legi generali*" (García Cavero, Percy. *Derecho penal económico. Parte general*. 4.ª edición. Lima: Instituto Pacífico, 2022, p. 718).

ideal[754]. *Lo mismo sucederá si dirigió un ataque que infectó decenas o cientos de computadoras para crear una red de bots (botnet)* y, de esta manera, controlarlas remotamente.

Una de las peculiaridades del delito de fraude informático es que su configuración, según el artículo 8 LDI[755], exige algún tipo de manipulación de datos informáticos (art. 3 LDI) o interferencia en el funcionamiento del sistema informático (art. 4 LDI). En este caso, el lector podrá apreciar que, en la legislación peruana, la manipulación de un sistema puede configurar una de las modalidades del fraude informático, por lo que nos encontramos frente a un concurso de leyes o concurso aparente de delitos. En aplicación del principio de consunción[756], el fraude informático absorbe el atentado contra la integridad de los datos o sistemas informáticos.

754 "Con el *nomen iuris* concurso ideal homogéneo se define la situación en que existe una identidad total, la cual tiene lugar cuando una sola conducta comunicativa quebranta varias veces una misma norma jurídico-penal de comportamiento [...]. Así, por ejemplo, existe concurso ideal homogéneo cuando una persona dispara a varias personas y les causa la muerte o cuando coloca una granada y mata a varias personas al mismo tiempo. En tal sentido, la diferencia sustancial entre un cumplimiento simple de los presupuestos del tipo penal y un concurso ideal homogéneo solo radica en el tenor diferente de la infracción de la norma de comportamiento. Un sector de la doctrina peruana considera que el Código Penal peruano no acepta el concurso ideal homogéneo; en su lugar, considera que, en dichos supuestos, existe un concurso ideal heterogéneo" (Salazar Sánchez, "Concurso ideal de delitos", cit., p. 37).

755 **LDI, Art. 8.-** El que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de **datos informáticos**, suplantación de interfaces o páginas web o cualquier interferencia o manipulación en el funcionamiento de un **sistema informático**, será reprimido [...] [El resaltado es mío].

756 "El principio de consunción se aplica en aquellos casos en los que la sanción prevista en un tipo penal engloba el supuesto de hecho de otro tipo penal bajo la lógica de un solo suceso conjunto. En tal caso, el tipo penal que consume el supuesto de hecho del tipo penal consumado desplaza a este último en su aplicación: *Lex consumens derogat legi consumptae*. En concreto, la consunción permite considerar dentro de la pena prevista para un delito determinado la pena que le correspondería a los hechos concomitantes (delito acompañante) o posteriores (delito posterior copenado) a la realización del tipo penal correspondiente. Es decir, se trata de actos vinculados al delito que, aunque pueden por sí mismos dar pie a un delito distinto, se consideran abarcados por la sanción penal prevista para el delito central" (García Cavero, *Derecho penal económico. Parte general*, cit., p. 719).

La Sala Penal Permanente, en el Recurso de Casación N.º 3330-2022, El Santa, del 14 de febrero del 2024, aludió este tópico, aunque no de forma explícita.

[Caso 101] Marco André Gómez, ejecutivo de banca personal del BBVA Banco Continental, utilizó documentos falsos (documentos de identidad y recibos de agua y luz) para manipular los sistemas informáticos del pago y, así, obtener doce tarjetas de crédito.

En este caso, si bien se discutió si existe concurso real o ideal entre el fraude informático y el uso de documento público falso, lo cierto es que existe una referencia a la alteración de datos o la manipulación del funcionamiento de los sistemas informáticos:

> **Quinto.** Que el otro motivo de casación, sustantivo en este caso, está en función a la subsunción jurídico penal de los hechos declarados probados. Concretamente, si se trata de un concurso real o de un concurso ideal de dos delitos: uso de documento público falso y fraude informático.
>
> [...]
>
> 3. El problema a discernir es si se está, dado el cuadro fáctico o histórico indicado *up supra*, ante una unidad de acción o ante una pluralidad de acciones, entendida desde una perspectiva normativa, a partir de las exigencias del tipo delictivo -el concurso ideal es una modalidad especial de la unidad de acción con una pluralidad de lesiones típicas de bienes jurídicos [...], seguidas por un solo fin o propósito [...]. En el caso *sub judice*, el imputado Gómez García, con los documentos falsos que recibió, tras manipular el sistema informático del Banco agraviado a partir del uso de tales documentos falsos, logró la obtención de tarjetas de crédito a nombre de los agraviados con las que se afectó patrimonialmente al Banco y a quienes se hizo aparecer como titulares de las tarjetas de crédito. **El tipo delictivo de fraude informático criminaliza la alteración de datos informáticos o la manipulación en el funcionamiento de un sistema**, y el tipo delictivo de falsedad material impropia castiga el mero uso de documentos falsos o falsificados. Es evidente, en el caso concreto, que el imputado utilizó los documentos en mención con los cuales manipuló el sistema informático;

> la utilización del documento falso se llevó a cabo precisamente para alterar o manipular el sistema informático. Se está, por tanto, ante una unidad de acción. [El resaltado es mío]
>
> 4. Como para la alteración o manipulación del sistema informático se usaron documentos falsos, es de aplicación el artículo 48 del Código Penal, según la Ley 28726, de nueve de mayo de dos mil seis; hubo una realización simultánea de dos tipos penales que no se excluyen entre sí [...]. La pena, en este caso, por tratarse de un concurso ideal de delitos, será hasta con el máximo de la pena privativa de libertad por el delito más grave. Pudiendo incrementarse esta hasta una cuarta parte. El delito más grave, en función a la pena privativa de libertad, es el de falsedad material impropia: hasta diez años de privación de libertad.

Ahora bien, en caso de que un ciberdelincuente atacase diversas plataformas estatales -como ocurrió en Costa Rica con el grupo Conti- durante un periodo específico, o dirigiese múltiples ataques de denegación de servicio (DoS) contra una empresa, estaríamos frente a un delito continuado. Otro ejemplo es el **Caso 90**, el cual analicé líneas arriba: un estudiante universitario empleó un USB Killer y lo utilizó para dañar 59 computadoras, el 14 de febrero de 2019.

[Caso 102] Sobre estos ejemplos, en nuestro país, la Corte Suprema de la República tuvo la oportunidad de analizar el siguiente caso de fraude informático: Un trabajador empleó un *skimmer* para clonar las tarjetas de crédito de los clientes de una entidad financiera, aprovechando que se encargaba del embolse de los plásticos que contenían dichas tarjetas. Al respecto, la Sala Penal Transitoria, en el Recurso de Nulidad N.º 557-2024, Lima, sostuvo que nos encontramos frente a un delito continuado:

> **Décimo cuarto.** Esta Suprema Sala Penal comparte la posición asumida por la Sala Penal Superior de que en el delito materia de imputación concurre la causal de incremento de la punibilidad regulada en el artículo 49 del CP. Sobre todo en atención con la pluralidad de sujetos perjudicados. Lo cual en el caso *sub iudice* se encuentra corroborado con el reporte de ingreso de reclamo y el memorando AI-001-2012, emitidos por el banco financiero (Banco Pichincha).

> De dichos documentos se advierten los diversos reclamos efectuados por los clientes entre los meses de setiembre a diciembre de 2011. Información que fue ratificada por Aldo Madruga Juárez, quien, en su condición de jefe de Prevención e Investigación de Fraudes del Banco Financiero (Banco Pichincha), determinó que de las 14 702 tarjetas emitidas entre setiembre y diciembre de 2011 se han reportado consumos inusuales en 88 tarjetas. De las cuales, los usuarios (tarjetahabientes) desconocen 375 operaciones de consumo ascendentes a S/ 254 657,26 y USD 27 468,05.
>
> [...]
>
> **Décimo séptimo.** Ahora bien, en atención a la pluralidad de personas perjudicadas y a lo establecido en el artículo 49 del Código Penal, así como en el fundamento 13 del Acuerdo Plenario 8-2009/CJ-116, este Supremo Tribunal considera que el extremo máximo incrementado de la pena conminada (incremento de un tercio de la máxima prevista para el hecho punible cometido) ahora es de 16 años de pena privativa de libertad.

7.12. PENALIDAD

En el delito de atentado a la integridad de sistemas informáticos, el autor será sancionado con pena privativa de libertad no menor a tres ni mayor a seis años y con ochenta a ciento veinte días-multa.

En este caso, he de replicar la crítica esgrimida sobre la proporcionalidad de la sanción, pues quien accede ilícitamente vulnerando las medidas de seguridad y quien atenta contra la integridad de los datos informáticos podría ser acreedor de la misma pena que el que atenta contra los sistemas, cuando esta última conducta reviste mayor gravedad. De ahí que la proporcionalidad de la pena no sea adecuada y merezca ser revisada.

7.13. CIRCUNSTANCIAS AGRAVANTES

Finalmente, son aplicables las cinco circunstancias previstas en el artículo 11 de la Ley N.º 30096:

i) Cometer el delito como integrante de una organización criminal.

[Caso 103] En esta publicación, he abordado tanto el crime as a service como el ransomware as a service como expresiones de la cibercriminalidad organizada. El impacto y daño que estas organizaciones es tal que, en el 2021, el FBI lanzó una campaña de recompensa en la ofrecía hasta diez millones de dólares por la captura de los líderes del grupo de *ransomware* REvil Sodinokibi.[757] En aquel entonces, dicho grupo atacó a más de mil empresas del sector industrial, generando millonarias pérdidas.

757 Sobre este punto, el FBI indicó lo siguiente: "La variante del *ransomware* Sodinokibi apareció inicialmente en abril de 2019 y desde entonces ha victimizado a más de 1.000 entidades en múltiples sectores industriales, incluyendo empresas privadas, agencias de aplicación de la ley, agencias gubernamentales e instituciones educativas y médicas. Un incidente de *ransomware* reciente y muy publicitado que se perpetró utilizando el Sodinokibi RaaS fue el de JBS Foods, un gran proveedor de productos agrícolas principalmente a Australia y Estados Unidos. El incidente afectó al 98 por ciento de su red de más de 5.000 servidores y causó una gran interrupción en el procesamiento y la entrega de alimentos. Además, Sodinokibi RaaS se utilizó para llevar a cabo un ataque contra Kaseya, una empresa de gestión de TI que proporciona servicios de red, aplicaciones e infraestructura a miles de pequeñas empresas y proveedores de servicios gestionados. El ataque de Kaseya no solo impactó las operaciones de Kaseya, sino también las de sus clientes en todo el mundo" [traducción propia], publicado el 8 de noviembre de 2021. https://www.state.gov/transnational-organized-crime-rewards-program-2/sodinokibi-ransomware-as-a-service-raas/

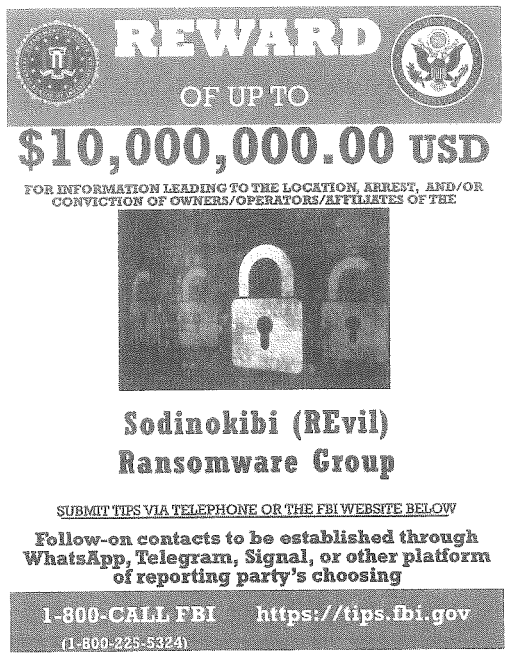


Imagen 24. Póster difundido por el FBI contra la ciberorganización criminal REvil Sodinokibi[758].

La organización fue desarticulada gracias a una operación internacional denominada QuickSand, liderada por la Interpol y con la colaboración de empresas del sector privado como Trend Micro, Kaspersky Lab y Palo Alto Networks, las cuales aportaron conocimientos técnicos e información clave. Asimismo, la empresa Bitdefender participó desarrollando herramientas que permitieron desencriptar sistemas infectados, lo que ayudó a 1400 empresas y evitó pérdidas estimadas en 475 millones de euros[759].

ii) Cometer el delito mediante el abuso de una posición especial de acceso a la data o información reservada o al conocimiento de esta información en razón del ejercicio de un cargo o función.

758 Fecha de consulta: 28 de febrero de 2025. Disponible en: https://www.amazon.com/-/es/USB-Kill-Pro-Kit-Estándar/dp/B06ZZS7NFS

759 Interpol. "Una operación mundial conjunta contra el ransomware se salda con detenciones y el desmantelamiento de una red delictiva", 8 de noviembre de 2021. https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2021/Una-operacion-mundial-conjunta-contra-el-ransomware-se-salda-con-detenciones-y-el-desmantelamiento-de-una-red-delictiva

iii) Cometer el delito con la finalidad de obtener un beneficio económico.

[Caso 104] En Madrid, se sentenció a un grupo de personas por distribuir mensajes falsos de la policía española, en los que se requería un pago de 100 euros. Cuando las víctimas ingresaban al enlace distribuido, descargaban un malware que encriptaba sus sistemas y ofrecían descifrarlo a cambio de dinero. En España, se identificaron 300 víctimas y los acusados fueron condenados[760]. Me parece muy interesante el esquema que se describe en la sentencia:

1. Creación y distribución del código malicioso
- El *ransomware* code era el encargado de programar el *malware* y ponerlo a disposición de otros miembros, sea por un monto específico o por un porcentaje de las ganancias.

2. Explotación del *ransomware*
- Los *ransomware* exploiters establecen la infraestructura de dominios y servidores para su propagación.

3. La infraestructura
- Los servidores de control C&C llevan el control estadístico de los usuarios infectados.

4. La infección
- Se realizaba a través de páginas web visitadas por las víctimas.

5. Movimiento económico del dinero obtenido
- Algunos miembros de la organización convertían el dinero UKASH, PaysafeCard o MoneyPak en dinero físico o virtual.

Esquema 6. Puesta en marcha y explotación del *ransomware*, descrito en la Sentencia N.º 14/16 del 3 de marzo de 2016. Elaboración propia.

iv) Comprometer fines asistenciales, la defensa, la seguridad y la soberanía nacionales.

[Caso 105] El grupo de cibercriminales CloAk Ransomware inició sus actividades ilegales entre fines del 2022 e inicios del 2023. Inicialmente, sus ataques se dirigieron a países de Europa, entre ellos, Alemania. Sin embargo, a fines del 2024, el Fuero Militar Policial[761] habría sido víctima de un ataque de secuestro informá-

760 SAN 704/2016. Sentencia N.º 14/16 del 3 de marzo de 2016, emitida por el Juzgado de Instrucción N.º 3 de la Audiencia Nacional. Sala de lo Penal de Madrid. Ponente: Carmen González Pastor.

761 El 22 de febrero de 2025, el suscrito visitó la web https://www.gob.pe/fmp, que pertenece al gobierno. Sin embargo, al dar clic a la opción "Visita su página oficial",

tico. Aunque las fuentes oficiales se limitaron a señalar que "una entidad pública" habría sido el objeto de ataque, en redes sociales se identificó al Fuero como la víctima en referencia:

> El grupo en referencia administra un sitio web donde vende o filtra los datos obtenidos de sus víctimas. En este caso, se habrían comprometido 221 GB de información, los cuales –según los portales consultados– habrían sido vendidos. Como se puede apreciar, nos encontramos frente a un grupo de ciberdelincuentes que secuestrarían sistemas informáticos con la finalidad de obtener algún beneficio económico de su ilícita actuación, pero que, en este caso particular, podría comprometer la seguridad nacional por la información a la cual accedió.

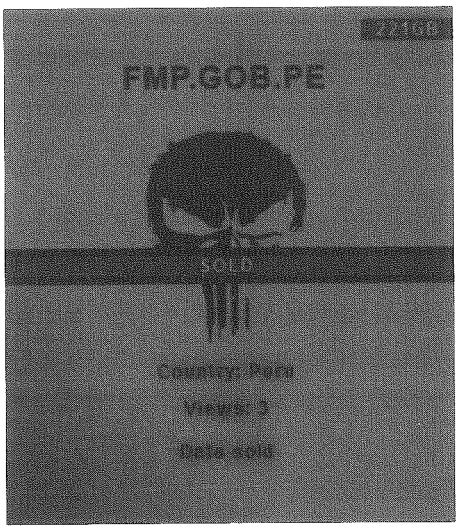


Imagen 25. Los ciberdelincuentes de la organización CloAk Ransomware dieron a conocer su ataque con esta ilustración[762].

no pudo acceder, ya que aparecía el siguiente mensaje: "Not Found. HTTP Error 404. The requested resource is not found".

762 Centro Nacional de Seguridad Digital. *Alerta integrada de seguridad digital* N.º 261-2024. Lima: 12 de noviembre de 2024, p. 4. https://www.gob.pe/institucion/pcm/informes-publicaciones/6174849-alerta-integrada-de-seguridad-digital-n-

v) Cometer el delito empleando la inteligencia artificial o tecnologías similares o análogas (conforme a la Ley N.º 32314).

7.14. PROPUESTA NORMATIVA

Tanto el Convenio de Budapest como la Convención de las Naciones Unidas contra la ciberdelincuencia recomiendan que se sancionen aquellas conductas que generen un resultado **grave**, elemento ausente en la legislación penal peruana actual. Considero adecuada esta inclusión, pues facilitará la labor jurisdiccional al sancionar únicamente las conductas que generen daños significativos.

En esta línea, en el siguiente pronunciamiento español se mencionan aquellos casos en los que no es necesario sancionar penalmente al autor ante la levedad o insignificancia del resultado generado por su conducta:

> Ahora bien, cuando el ataque únicamente produce una interrupción intermitente de la página web que quedó fuera de servicio en intervalos de minutos y el problema quedó resuelto en una hora, el correo electrónico siguió funcionando y los perjuicios derivados de los hechos inicialmente estimados en setecientos euros no eran tales porque el trabajo lo realizó un empleado en nómina al que no se le abonó cantidad alguna por dicho servicio, entonces se produce la atipicidad del suceso (SJP N.º 3 de Gijón, de 6 de julio de 2016)[763].

Dicho esto, y a partir del análisis expuesto en este capítulo, propongo modificar el delito de atentado a los sistemas informáticos, tomando en consideración:

i. Reformar el *nomen iuris* del delito actualmente denominado *atentado a la integridad de datos informáticos*, sustituyéndolo por *ataque a la integridad y disponibilidad de los sistemas informáticos*.

261-2024-cnsd. Además, las cuentas de ciberseguridad @TMRansomMon, @Treadstone71LLC y @V3n0mStrike, lo reportaron el 20 y el 22 de diciembre de 2024, respectivamente. Las publicaciones pueden ser visualizadas en los siguientes enlaces: https://x.com/tmransommon/status/1870074567449854087?s=61 https://x.com/treadstone71llc/status/1869991934535623080?s=61 https://x.com/v3n0mstrike/status/1870837068198293514?s=61

763 Barrio Andrés, *Delitos 2.0. Aspectos penales, procesales y de seguridad de los ciberdelitos*, cit., p. 116.

ii. Eliminar los elementos *deliberada* e *ilegítimamente*.

iii. Precisar que la afectación debe ser el resultado de introducir, transmitir, dañar, borrar, deteriorar, alterar o suprimir datos informáticos.

iv. Precisar que la afectación al sistema informático debe ser *grave*.

v. Incrementar la sanción prevista, en atención a la gravedad que representa.

De este modo, el delito bajo estudio se regularía en los siguientes términos:

> **Art. 4.- Ataques a la integridad y disponibilidad de los sistemas informáticos**
>
> El que impide el acceso u obstaculiza gravemente el funcionamiento de un sistema informático, mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos será reprimido con pena privativa de libertad no menor de cinco ni mayor de diez años y con ochenta a ciento veinte días-multa.

7.15. CONCLUSIONES DEL CAPÍTULO

- Nuestra legislación penal se aleja significativamente de la regulación propuesta por el Convenio de Budapest en lo que al delito de atentado contra los sistemas informáticos se refiere. Mientras que este último exige una obstaculización grave del funcionamiento del sistema informático originada por actos como la introducción, borrado o alteración de datos, la normativa peruana omite la exigencia de gravedad y no vincula expresamente el ataque al tratamiento de datos. Esta omisión genera una formulación ambigua del tipo penal, dificultando su correcta interpretación y aplicación práctica.
- El tipo penal recogido en el artículo 4 de la LDI utiliza verbos rectores como *inutilizar*, *impedir el acceso*, *entorpecer* o *imposibilitar*, apartándose del Convenio de Budapest. Esta técnica legislativa deficiente dificulta su subsunción en los casos concretos, originando inseguridad jurídica. La ausencia de un criterio de gravedad, como el que exige el citado Convenio, incrementa el riesgo de sobrecriminalización de las conductas.

- El análisis de la legislación de diversos países evidencia la disparidad terminológica y conceptual en torno al delito de atentado contra sistemas informáticos. Mientras algunos ordenamientos lo ubican en capítulos vinculados al patrimonio, otros lo hacen en el marco de la seguridad informática. Esta diversidad revela la falta de un consenso internacional y refuerza la necesidad de armonizar conceptos clave como *sistema informático*, *obstaculización* y *gravedad*, a fin de consolidar una respuesta penal coherente frente a este tipo de ciberdelitos.
- Contrario a posturas doctrinarias que exigen conocimientos técnicos avanzados para configurar la autoría del delito, la legislación local y comparada considera que se trata de un delito común, es decir, puede ser cometido por cualquier persona. La proliferación de herramientas en el mercado negro -como *malware* prefabricado o servicios de ataque- confirma que incluso individuos con conocimientos limitados (*script kiddies*) pueden llevar a cabo ataques cibernéticos graves.
- En este capítulo se resalta la distinción entre los ataques dirigidos contra el componente físico (*hardware*) y aquellos que afectan el componente lógico (*software*) de un sistema. Esta diferencia es crucial para delimitar si se está ante un delito de daños previsto en el Código Penal o ante un atentado a la integridad del sistema informático, tipificado en la LDI. Casos como el del uso del USB Killer exponen las zonas grises donde ambos tipos podrían superponerse, requiriendo un análisis técnico y jurídico más profundo.
- A diferencia de lo propuesto en el Convenio de Budapest o en la Convención de las Naciones Unidas contra la Ciberdelincuencia, la legislación peruana no contempla de forma explícita los medios mediante los cuales se perpetra el ataque (como la introducción, transmisión, alteración de datos), lo cual constituye una omisión relevante.
- A la luz del análisis dogmático, comparado y jurisprudencial, se evidencia que nuestra legislación requiere una reforma integral. Esta debería incorporar el criterio de gravedad, definir de manera técnica los verbos rectores, precisar el medio comisivo y armonizar la terminología con la legislación comparada. Solo de este modo se podrá garantizar una protección efectiva del bien jurídico frente a las nuevas amenazas digitales.

CAPÍTULO 8

INTERCEPTACIÓN ILÍCITA DE DATOS INFORMÁTICOS



* La ilustración de la página anterior corresponde a una adaptación de *Mujer leyendo una carta*, de Gabriël Metsu (1662-1665). Para su elaboración, se empleó una de las herramientas de generación de imágenes de la empresa OpenAI.

CAPÍTULO 8

INTERCEPTACIÓN ILÍCITA DE DATOS INFORMÁTICOS

Sumario: 8.1. Introducción. 8.2. Regulación en el Convenio sobre la Ciberdelincuencia. 8.3. Regulación en la Convención de las Naciones Unidas contra la Ciberdelincuencia. 8.4. Legislación comparada. 8.5. Legislación nacional. 8.6. El bien jurídico penalmente protegido. 8.7. Tipicidad objetiva. 8.8. Tipicidad subjetiva. 8.9. Las situaciones de justificación en el delito de interceptación ilícita de datos informáticos. 8.10. Consumación. 8.11. Concursos. 8.12. Penalidad. 8.13. Circunstancias agravantes. 8.14. Propuesta normativa. 8.15. Conclusiones del capítulo.

Nos vigilan. Saben que estoy escribiendo estas palabras. Saben que las estás leyendo. Gobiernos y cientos de empresas nos espían: a ti, a mí y a todos nuestros conocidos. Cada minuto, todos los días. Rastrean y registran todo lo que pueden: nuestra ubicación, nuestras comunicaciones, nuestras búsquedas en internet, nuestra información biométrica, nuestras relaciones sociales, nuestras compras y mucho más. Quieren saber quiénes somos, qué pensamos, dónde nos duele. Quieren predecir nuestro comportamiento e influir en él. Tienen demasiado poder. Su poder provine de nosotros, de ti, de tus datos. Es hora de volver a tomar el control. Recuperar la privacidad es la única manera de que podamos asumir de nuevo el mando de nuestra vida y de nuestras sociedades.

Internet se financia principalmente mediante la recopilación, el análisis y el comercio de datos: la economía de los datos. Muchos de ellos son personales: datos de ti. La compraventa de estos datos personales como modelo de negocios se está exportando a cada vez más instituciones de la sociedad que pasa a ser la sociedad (o el capitalismo) de la vigilancia[764].

764 Véliz, *Privacidad es poder. Datos, vigilancia y libertad en la era digital,* cit., p. 11.

8.1. INTRODUCCIÓN

Este delito es conocido como *espionaje informático* y se encuentra recogido tanto en el artículo 3 del Convenio de Budapest como en el artículo 8 de la Convención de las Naciones Unidas contra la Ciberdelincuencia. Ciertamente, el contenido de la información a la que se puede acceder es muy peligrosa, pudiendo exponer la seguridad nacional. Por esta razón, algunos ordenamientos, como el peruano, incluyen circunstancias agravantes según la información obtenida.

Nuestro Código Penal sanciona el delito de interferencia telefónica (art. 162) y el delito de interferencia de comunicaciones electrónicas, de mensajería instantánea y similares (art. 162-B), por lo que el ilícito de interceptación ilegal de datos complementa las conductas que deben ser sancionadas a fin de evitar espacios de impunidad.

En ciertos casos, este delito se utiliza como medio para obtener credenciales bancarias que luego son empleadas en fraudes informáticos. No obstante, también observamos que algunas agencias gubernamentales acceden a información confidencial, moviéndose en una delgada línea que separa lo legal de lo ilegal.

[Caso 106] El AirHopper es un *malware* tipo *keylogger* que *graba* las pulsaciones de teclas y las recoge en un archivo. Es capaz de recibir ciertas señales de radio que emiten ciertos modelos de monitor o pantalla. Para ello emplea ondas de radio FM con las que se puede transmitir una señal que será recogida y almacenada por un receptor. Así, permite robar claves o mensajes privados. La señal se traduce y almacena pudiendo ver en tiempo real lo que el usuario está escribiendo en el otro dispositivo[765].

[Caso 107] La empresa israelí NSO Group desarrolló un *software* espía denominado Pegasus. La función principal era infectar *smartphones* y, sin que el usuario lo sepa, extraer información. La citada empresa ha señalado que el *spyware* fue vendido a entidades gubernamentales para fortalecer la

765 Gil Gil y Hernández Berlinches, *Cibercriminalidad,* cit., p. 208.

lucha contra la criminalidad, especialmente contra la criminalidad terrorista. Sin embargo, sus descargos no la libraron de innumerables críticas e investigaciones a nivel mundial.

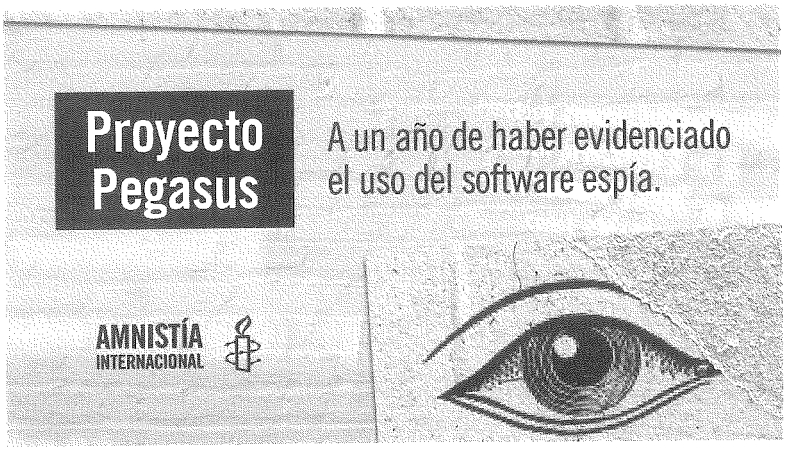


Imagen 26. Amnistía Internacional ha cuestionado la comercialización de *softwares* espías como Pegasus[766].

En el 2022, el instituto canadiense Citizen Lab informó que tres docenas de periodistas y activistas de El Salvador habrían sido afectados entre julio de 2020 y noviembre de 2021[767]. Sin embargo, un año antes, Amnistía Internacional ya había advertido sobre su uso. En el documento titulado Forensic Methodoly Report: How to catch NSO Group Pegasus[768]. De este modo, se identificaron casos que involucraban a periodistas, políticos, abogados y activistas de Marruecos, Francia, Hungría, India, Azerbaiyán, México, Emiratos Árabes Unidos, Ruanda y Arabia Saudita. Se estima que habrían más de 50 mil números telefónicos comprometidos.

766 La imagen fue descargada de: Amnistía Internacional. "Proyecto Pegasus: Un año después, la crisis de los programas espía continúa, mientras el sector de la vigilancia sigue sin estar sometido a control", 20 de julio de 2022. https://amnistia.org.uy/proyecto-pegasus-un-ano-despues/

767 "El hackeo a gran escala con un programa israelí a periodistas y activistas de El Salvador", en *BBC*, 13 de enero de 2022. https://www.bbc.com/mundo/noticias-america-latina-59985209

768 El informe, en inglés, puede ser descargado en: https://www.amnesty.org/en/documents/doc10/4487/2021/en/

Los casos expuestos no serían los únicos, pues, en el 2024, el presidente colombiano Gustavo Petro informó que el gobierno de su predecesor habría adquirido el *spyware* en pagos que ascendía a 11 millones de dólares[769].

Como se puede apreciar, la afectación de datos informáticos representa una amenaza real, lo que justifica y motiva un análisis detallado de sus diversas modalidades y de las respuestas que ofrecen las legislaciones al respecto.

8.2. REGULACIÓN EN EL CONVENIO SOBRE LA CIBERDELINCUENCIA

El artículo 3 del Convenio de Budapest regula el delito de interceptación ilícita en los siguientes términos:

> **Art. 3.- Interceptación ilícita**
>
> Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la interceptación deliberada e ilegítima por medios técnicos de datos informáticos en transmisiones no públicas dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos. Las Partes podrán exigir que el delito se cometa con intención delictiva o en relación con un sistema informático conectado a otro sistema informático.

La fórmula legislativa propuesta en el Convenio puede graficarse de la siguiente forma:

769 "Colombia to investigate police purchase of Pegasus spyware", en *BBC*, 5 de setiembre de 2024. https://www.bbc.com/news/articles/ckg5en18qvxo

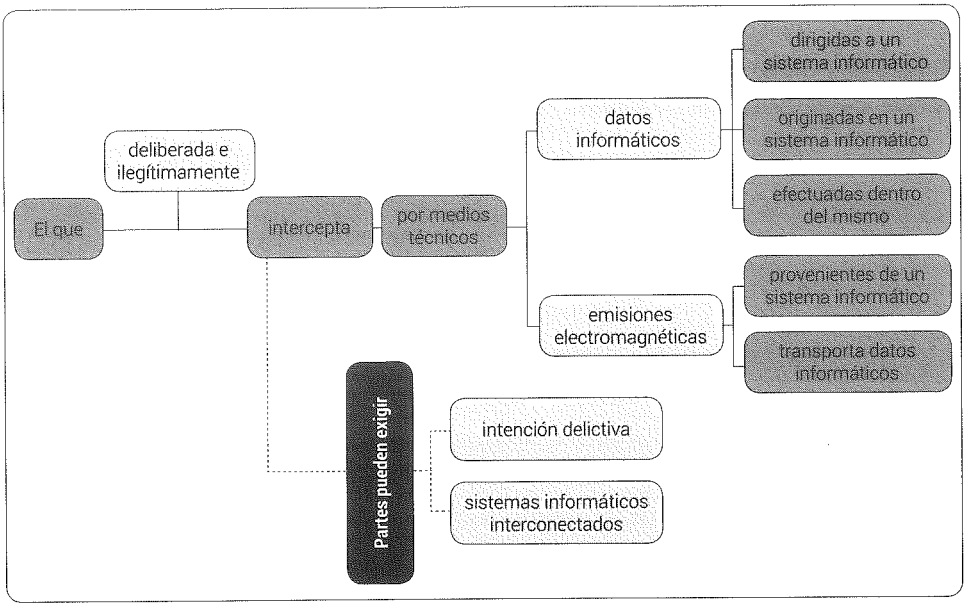


Diagrama 17. Estructura del delito de interceptación ilícita, propuesto en el Convenio de Budapest. Elaboración propia.

Es importante apreciar que sistemáticamente se ubica después del delito de acceso ilícito. Considero que esto no es una coincidencia, sino que la legislación es armónica, ya que el objeto de protección de ambos delitos es la confidencialidad de los datos y sistemas informáticos.

Ahora bien, los párrafos 51 a 59 del Informe Explicativo del Convenio de Budapest permite comprender los alcances del tipo penal bajo estudio:

- En el párrafo 51 se precisa que se tutela el derecho a la privacidad de las comunicaciones de datos y compara este ilícito con interceptaciones tradicionales, como la intervención y grabación de las conversaciones telefónicas orales entre las personas. Además, alude al artículo 8 de la Convención Europea de Derechos Humanos y recuerda que la protección de este delito sanciona cualquier tipo de transferencia electrónica de datos, ya sea por teléfono, fax, correo electrónico o transferencia de archivos. Es importante destacar que no menciona el derecho a la intimidad -aspecto que destacaré al analizar el bien jurídico penalmente protegido-.

- En el párrafo 52 se aclara que las comunicaciones involucradas están relacionadas con las transmisiones de datos informáticos, así como con las radiaciones electromagnéticas.
- En el párrafo 53 se destaca la importancia de los medios técnicos en la comisión de este delito -elemento que no ha sido contemplado en la normativa peruana-. Bajo esta premisa se incluyen dispositivos conectados a las líneas de transmisión, así como los dispositivos utilizados para obtener y gabar las comunicaciones inalámbricas. De este modo, claramente se indica que pueden incluir el uso de *software*, contraseñas y códigos. Este apartado también desarrolla los alcances del verbo *interceptar*: escuchar, monitorear o vigilar el contenido de las comunicaciones y adquirir los contenidos de datos -directa o indirectamente, como se desarrollará más adelante-.

  Lamentablemente, el legislador peruano no tomó en consideración el elemento *medios técnicos*, aspecto importante, pues el propio Informe Explicativo así lo señala: "El requisito de que se utilice un medio técnico es una matización restrictiva destinada a evitar que se establezcan demasiados delitos".
- En el párrafo 54 se explica que el delito alcanza las transmisiones *no públicas* de datos informáticos, pero precisa que se refiere a la naturaleza del proceso de transmisión y no a la naturaleza de los datos transmitidos. De este modo, dichos datos pueden girar en torno a información que esté accesible al público, pero que las partes quieren comunicar de forma confidencial. El Informe Explicativo señala que las partes, con fines comerciales, desean mantener en secreto la información hasta que se pague por el servicio -como sucede en el servicio de televisión de previo pago o *pay per view*-.
- El párrafo 55, en línea con los anteriores, se precisan los tipos de comunicación que pueden producirse al interior de un único sistema informático -transmitiendo información del CPU a la pantalla o a la impresora-, entre dos sistemas informáticos que pertenecen a una misma persona, entre dos ordenadores que se comunican entre sí, o entre un ordenador y una persona. Si bien el Informe Explicativo indica que las partes podrán exigir como elemento adicional que la comunicación sea transmitida entre sistemas in-

formáticos que estén conectados de forma remota, la legislación peruana tutela de forma amplia los diferentes tipos de transmisión que pueden producirse.

- En el párrafo 56 se precisa que las partes no tienen la obligación de establecer como delito la interceptación de cualquier transmisión como, por ejemplo, las de radio. De este modo, cada parte analizará si reprime a los radioaficionados que intercepten transmisiones abiertas y de fácil acceso. Perú no hace distinción alguna ni formuló reserva en este tópico.
- En el párrafo 57 se señala que las emisiones electromagnéticas no son datos informáticos, según la definición descrita en el artículo 1 del Convenio de Budapest, sin embargo, su tutela es importante teniendo en cuenta que los datos pueden ser reconstruidos a partir de dichas emisiones.
- En el párrafo 58 se recuerda que la conducta debe ser deliberada e ilegítima. Sobre este último elemento, se brindan algunos ejemplos de conductas permitidas: si quien intercepta los datos informáticos tiene permiso para hacerlo, si actúa bajo las órdenes o con la autorización de los participantes en la transmisión o si la vigilancia corresponde a asuntos de seguridad nacional o la detección de delitos por parte de las autoridades que los investigan.

  Este párrafo precisa que los usos de prácticas comerciales comunes como el empleo de *cookies* no constituyen interceptaciones ilícitas.
- Finalmente, en el párrafo 59 se establece que la interceptación de datos puede estar relacionada estrechamente con el delito de acceso ilícito o intrusismo informático. Por esta razón, las partes pueden establecer matices en la redacción de ambos delitos.

Perú, al adherirse al Convenio de Budapest, declaró que nuestra "legislación exige que el delito de interceptación se cometa con intención delictiva y que dicho delito pueda cometerse en relación con un sistema informático conectado a otro sistema informático".

8.3. REGULACIÓN EN LA CONVENCIÓN DE LAS NACIONES UNIDAS CONTRA LA CIBERDELINCUENCIA

El artículo 8 de la Convención regula el delito de interceptación ilícita en los siguientes términos:

> **Art. 8.- Interceptación ilícita**
>
> 1. Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para tipificar como delito en su derecho interno la interceptación deliberada y sin derecho, por medios técnicos, de transmisiones no públicas de datos electrónicos en un sistema de tecnología de la información y las comunicaciones, desde él o dentro de él, incluidas las emisiones electromagnéticas provenientes de un sistema de tecnología de la información y las comunicaciones que transporten esos datos electrónicos.
> 2. Los Estados partes podrán exigir como requisito que el delito se cometa con intención deshonesta o delictiva o en relación con un sistema de tecnología de la información y las comunicaciones que esté conectado a otro sistema de tecnología de la información y las comunicaciones.

La redacción es similar a la adoptada en el Convenio de Budapest. Los cambios son mínimos, pues, como ya se ha explicado, reemplazan la expresión *sistemas informáticos* por *sistemas de tecnología de la información y las comunicaciones*, así como la expresión *datos informáticos* por *datos electrónicos*. Además, se aprecian ligeros cambios en el orden de presentación de los elementos del tipo penal, que no afectan sus alcances.

8.4. LEGISLACIÓN COMPARADA

País	Legislación	Tipo penal
Países latinoamericanos que se adhirieron al Convenio de Budapest		
Ecuador	**Código Orgánico Integral Penal**	**Sección Tercera. Delitos contra la seguridad de los activos de los sistemas de la información y comunicación** **Art. 230.- Interceptación ilegal de datos.-** Será sancionada con pena privativa de libertad de tres a cinco años: 1. La persona que, sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma, contenido digital en su origen, destino o en el interior de un sistema informático o dispositivo electrónico, una señal o una transmisión de datos o señales. [...]

País	Legislación	Tipo penal
Brasil	**Lei N.º 9 296**	**Lei N.º 9296** **Art. 10.-** Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, promover escuta ambiental ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei: Pena - reclusão, de 2 (dois) a 4 (quatro) anos, e multa. **Art. 10-A.-** Realizar captação ambiental de sinais eletromagnéticos, ópticos ou acústicos para investigação ou instrução criminal sem autorização judicial, quando esta for exigida: Pena - reclusão, de 2 (dois) a 4 (quatro) anos, e multa.
Colombia	**Código Penal**	Título VII-A. De delitos contra el patrimonio cultural sumergido **Art. 269 C.- Interceptación de datos informáticos** El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.
Paraguay	**Código Penal**	**Capítulo VII. Hechos punibles contra el ámbito de la vida y la intimidad de la persona** **Art. 146 C.-** Interceptación de datos El que, sin autorización y utilizando medios técnicos: 1. obtuviere para sí o para un tercero, datos en sentido del Art. 146 b, inciso 2º, no destinados para él; 2. diera a otro una transferencia no pública de datos; o 3. transfiriera la radiación electromagnética de un equipo de procesamiento de datos, será castigado con pena privativa de libertad de hasta dos años o multa, salvo que el hecho sea sancionado por otra disposición con una pena mayor.
Argentina	**Código Penal**	**Capítulo III. Violación de secretos y de la privacidad** **Art. 153.-** Será reprimido con prisión de quince (15) días a seis (6) meses el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida. En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido. La pena será de prisión de un (1) mes a un (1) año, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica. Si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá, además, inhabilitación especial por el doble del tiempo de la condena.
Costa Rica	**Código Penal**	**Sección I. Violación de secretos. Violación de correspondencia** **Art. 196.- Violación de correspondencia o comunicaciones** Será reprimido con pena de prisión de uno a tres años a quien, con peligro o daño para la intimidad o privacidad de otro, y sin su autorización, [...] intervenga, intercepte [...] documentación o comunicaciones dirigidas a otra persona. [...] La misma pena se impondrá a quien promueva, incite, instigue, prometa o pague un beneficio patrimonial a un tercero para que ejecute las conductas descritas en los dos párrafos anteriores. La pena será de dos a cuatro años de prisión si las conductas descritas en el primer párrafo de este artículo son realizadas por: a) Las personas encargadas de la recolección, entrega o salvaguarda de los documentos o comunicaciones. b) Las personas encargadas de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tengan acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.

País	Legislación	Tipo penal
Costa Rica	Código Penal	**Art. 196 *bis*.- Violación de datos personales** Será sancionado con pena de prisión de tres a seis años quien en beneficio propio o de un tercero, con peligro o daño para la intimidad o privacidad y sin la autorización del titular de los datos, [...] interfiera, [...] transmita, [...] intercepte, [...] desvíe para un fin distinto para el que fueron recolectados o dé un tratamiento no autorizado a las imágenes o datos de una persona física o jurídica almacenados en sistemas o redes informáticas o telemáticas, o en contenedores electrónicos, ópticos o magnéticos. La pena será de cuatro a ocho años de prisión cuando las conductas descritas en esta norma: a) Sean realizadas por personas encargadas de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tengan acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos. b) Cuando los datos sean de carácter público o estén contenidos en bases de datos públicas. c) Si la información vulnerada corresponde a un menor de edad o incapaz. d) Cuando las conductas afecten datos que revelen la ideología, la religión, las creencias, la salud, el origen racial, la preferencia o la vida sexual de una persona.
Chile	Ley N.° 21459	**Título I. De los delitos informáticos y sus sanciones** **Art. 3.- Interceptación ilícita** El que indebidamente intercepte, interrumpa o interfiera, por medios técnicos, la transmisión no pública de información en un sistema informático o entre dos o más de aquellos, será castigado con la pena de presidio menor en su grado medio. El que, sin contar con la debida autorización, capte, por medios técnicos, datos contenidos en sistemas informáticos a través de las emisiones electromagnéticas provenientes de éstos, será castigado con la pena de presidio menor en sus grados medio a máximo.
Panamá	Código Penal	**Título I. De los delitos informáticos y sus sanciones** **Art. 290.-** Quien indebidamente se apodere, copie, utilice o modifique los datos en tránsito o contenidos en una base de datos o sistema informático, o interfiera, intercepte, obstaculice o impida su transmisión será sancionado con dos a cuatro años de prisión.
República Dominicana	Ley N.° 53-07	**Capítulo I. Crímenes y delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos** **Art. 9.- Interceptación e intervención de datos o señales** El hecho de interceptar, intervenir, injerir, detener, espiar, escuchar, desviar, grabar u observar, en cualquier forma, un dato, una señal o una transmisión de datos o señales, perteneciente a otra persona por propia cuenta o por encargo de otro, sin autorización previa de un juez competente, desde, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones, o de las emisiones originadas por éstos, materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas físicas o morales, se sancionará con la pena de uno a tres años de prisión y multa de veinte a cien veces el salario mínimo, sin perjuicio de las sanciones administrativas que puedan resultar de leyes y reglamentos especiales.
Otras referencias		
España	Código Penal	**Capítulo IX. De los daños** **Art. 197 *bis*.-** 2. El que mediante la utilización de artificios o instrumentos técnicos, y sin estar debidamente autorizado, intercepte transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información, incluidas las emisiones electromagnéticas de los mismos, será castigado con una pena de prisión de tres meses a dos años o multa de tres a doce meses.

Cuadro 27. Legislación comparada respecto al delito de interceptación ilícita de datos informáticos. Elaboración propia.

El delito de interceptación ilegal de datos informáticos se encuentra ubicado en diferentes capítulos, según la legislación analizada. De este modo, Colombia y España lo sitúan en el acápite de los delitos contra el patrimonio o daños; Argentina, Costa Rica y Paraguay, en cambio, lo ubican en capítulos como violación de secretos o correspondencia, violación de secretos y privacidad e ilícitos contra la vida personal e intimidad. Finalmente, algunas legislaciones, como las de Chile, Ecuador, Panamá y República Dominicana, lo sitúan en capítulos afines a la seguridad informática.

Chile, España y Paraguay precisan que la interceptación de datos informáticos debe realizarse mediante artificios o instrumentos técnicos, siguiendo, de esta forma, la recomendación del Convenio de Budapest.

Interceptar es el verbo rector sugerido en el Convenio, sin embargo, las legislaciones han agregado diferentes modalidades: *intervenir, injerir, detener, espiar, escuchar, desviar, grabar* u *observar*. La legislación española es la más cercana a lo propuesto en la fórmula internacional.

Chile, Colombia, España y Paraguay[770] incluyen, además de los datos informáticos, la interceptación de emisiones electrónicas. De este modo, cubren un abanico de posibilidades mucho más amplio que otras regulaciones.

8.5. LEGISLACIÓN NACIONAL

8.5.1. Antecedentes normativos

Solo un proyecto de ley sugirió la incorporación de la interceptación de datos informáticos, sin embargo, la fórmula legal lo incluyó como parte del delito de acceso ilícito:

- **Proyecto de Ley N.º 5132/99-CR,** presentado el 31 de agosto de 1999 por la congresista Susana Díaz Díaz[771]. Se propuso la tipificación de un delito que sancionara tanto la interceptación como el acceso (intrusismo informático) y la interferencia (espionaje in-

770 Paraguay utiliza la expresión *radiación electromagnética*.

771 **Proyecto de Ley N.º 5132/99-CR, art. 2.-** El que, con ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte [...] será reprimido con pena privativa de libertad no mayor de tres años.

formático). Esta propuesta no prosperó, pero se incluyó el vocablo *interceptar* como una de las finalidades delictivas perseguidas a través del primigenio acceso ilícito.

A fines del siglo XX, nuestro legislador ya se preocupaba por la interceptación de datos informáticos. Evidencia de ello es la sesión parlamentaria del 3 de mayo de 2000, en la que se debatió un texto sustitutorio, contenido en el dictamen unánime de la Comisión de Reforma de Códigos. En el debate, el congresista Díez-Canseco Cisneros advirtió la necesidad de sancionar estas novedosas conductas ilícitas, ejemplificándolo con el ciberataque sufrido por uno de nuestros parlamentarios:

> El día de hoy ha juramentado el congresista García-Sayán, quien podría dar testimonio ante el Pleno del Congreso de cómo el correo electrónico a través del cual se manejaron los mecanismos en la búsqueda de una candidatura unitaria fue objeto de interceptación y luego de publicación en el diario *Expreso* -si no me equivoco-, que tanto defiende determinados principios y determinados intereses políticos del país. De manera que esta es una iniciativa que llega con relativo retraso al Pleno, en la medida en que mecanismos de esta naturaleza han venido siendo utilizados en forma notaria y escandalosa en nuestro país.

En esta línea, el referido parlamentario señaló que debía mejorarse la redacción de la fórmula legislativa en tanto "se coloca en un mismo saco el hecho de interceptar una información en curso en una computadora y los objetivos por los cuales se produce la interceptación de la información" -reflexión similar a la esbozada línea arriba-. Así, concluyó lo siguiente:

> El proyecto de ley en debate no solo debería incrementar determinadas penalidades, sino también hacer diferencia entre las mismas. En ese sentido, un hecho que debe ser debidamente sancionado es la sola intervención de una comunicación de carácter privado, más allá de si existe un fin de obtención de dinero, o de un secreto comercial o industrial o bancario, o a obtención de un bien determinado. En ciertas circunstancias, y particularmente en lo que concierne al espionaje político, el único interés es la obtención estricta de la información, la cual en este ámbito se convierte en un bien valorado.

En el debate, el congresista Olivera Vega manifestó que estas conductas podrían subsumirse bajo el delito de violación del secreto de las comunicaciones, previsto en el artículo 162 CP:

> Creo que el ingresar a un banco de datos o a un archivo computarizado es algo semejante a una interceptación telefónica o a una violación del secreto de las comunicaciones. Aquí mismo, y esto lo saben algunos parlamentarios, se ha estado denunciando -y creo que en un momento dado el congresista Díez-Canseco hizo una denuncia similar- que con respecto a nuestro banco de datos de correspondencia en el Congreso habría un sistema de interceptación [...] **Creo que estos ilícitos penales perfectamente podrían ser comprendidos en el artículo 162** del Capítulo V del Código Penal, referido a la violación de secretos de las comunicaciones [...] [El resaltado es mío].

En dicha jornada se hizo un intermedio para delimitar los tipos penales propuestos. La incorporación autónoma del delito de interceptación de datos informáticos no fue propuesta -entiendo, porque los legisladores consideraron que no existía un vacío normativo, ya que el artículo 162 CP lo cubriría, en su opinión-. La norma en mención se encontraba redactada en los siguientes términos:

> **Art. 162.- Interferencia telefónica.** El que, indebidamente, interfiere o escucha una conversación telefónica o similar será reprimido con pena privativa de libertad no menor de uno ni mayor de tres años.

8.5.2. Génesis legislativa

En Perú, la interceptación de datos informáticos se origina en tres proyectos de ley. En dos de ellos se proponen incluir este delito en el capítulo IV, denominado "Violación del secreto de las comunicaciones" del Código Penal, mientras que el otro, en una norma especial.

- **Proyecto de Ley N.º 00034/2011-CR**, presentado el 11 de agosto de 2011 por el congresista Juan Carlos Eguren Neuenschwan-

der[772]. Esta propuesta recoge tanto modalidades del acceso ilícito (*acceder*) como de ataques contra datos y sistemas informáticos (*interferir, modificar, desviar, eliminar*). De este modo, la técnica legislativa adoptada resulta inadecuada. Pese a ello, es importante destacar que se establece el elemento por el cual se cometerá este ilícito: las TIC.

- **Proyecto de Ley N.° 01257/2011-CR**, presentado el 14 de junio de 2012 por el congresista Tomás Zamudio Briceño, propuso incorporar el artículo 161-A CP[773]. En este caso, no se establece el elemento con el que se comete el ilícito -empleándose una fórmula abierta-. Además, recoge diferentes modalidades para su configuración: conocer, sustraer, interceptar, interferir, cambiar o alterar (el texto), desviar el curso o facilitar que terceros conozcan la existencia o contenido de la comunicación. Adicionalmente, se propone sancionar con las mismas penas a quienes, por razón de su cargo, tienen conocimiento o acceden al contenido de una comunicación.
- **Proyecto de Ley N.° 02520/2012-PE**, presentado el 26 de julio de 2013 por el presidente de la República Ollanta Humala[774], pro-

772 **Proyecto de Ley N.° 00034/2011-CR, art. 9.-** ***Violación del secreto de las comunicaciones.*** El que, mediante el uso de tecnologías de información, accede, capture, intercepte, interfiera, reproduzca, modifique, desvíe o elimine cualquier mensaje de datos o señal de transmisión o comunicaciones ajenas, será reprimido con pena privativa de libertad no menor de dos ni mayor de cinco años.

773 **Proyecto de Ley N.° 01257/2011-CR, art. 161.-** ***Inviolabilidad del secreto de las comunicaciones.*** Será reprimido con la pena privativa de libertad no menor de 5 ni mayor de 15 años cuando deliberadamente una persona quien no es el que origina ni es el destinatario de la comunicación conoce, sustrae, intercepta, interfiere, cambia o altere su texto, desvíe su curso, o facilite que terceros conozcan la existencia o contenido de la comunicación.
Tendrán igual sanción las personas que en razón de su función tienen conocimiento o acceso al contenido de una comunicación cursada a través de los servicios públicos de comunicación.

774 **Proyecto de Ley N.° 02520/2012-PE, art. 162-A.-** ***Interceptación de datos informáticos.*** El que, a través de las tecnologías de la información o de la comunicación, intercepta datos informáticos en transmisiones no públicas, dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que

puso incluir el artículo 162-A CP. Esta propuesta normativa fue la que primó, ya que se adoptó íntegramente.

8.5.3. Evolución legislativa

Pocos meses después de la aprobación de la LDI, se modificó el delito de interceptación ilícita de datos informáticos. En esta ocasión, fueron tres los proyectos que recogieron el cambio incorporado mediante la Ley 30171:

- **Proyectos de Ley N.º 02991/2013-CR**, presentado el 25 de noviembre de 2013 por el congresista Juan Carlos Eguren Neuenschwander[775]. Este proyecto propuso (i) incluir los elementos *deliberada* e *ilegítimamente*, (ii) no incluir el medio comisivo y (iii) precisar la norma de remisión: la ley de transparencia y acceso a la información pública.
- **Proyecto de Ley N.º 02999/2013**, presentado el 27 de noviembre de 2013 por el congresista Mauricio Mulder Bedoya[776]. La fór-

---

transporta dichos datos informáticos, será reprimido con una pena privativa de libertad no menor de tres ni mayor de seis años.
La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con las normas de la materia.
La pena privativa de libertad será no menor de ocho ni mayor de diez años cuando el delito comprometa la defensa, seguridad o soberanía nacionales.

775 **Proyectos de Ley N.º 02991/2013-CR, art. 7.** ***Interceptación de datos informáticos.***- El que deliberada e ilegítimamente intercepta datos informáticos en transmisiones no públicas, dirigidas a un sistema informático, originados en un sistema informático o efectuado dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos, será reprimido con una pena privativa de libertad no menor de tres ni mayor de seis años.
La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con la Ley de Transparencia y acceso a la información pública.
La pena privativa de libertad será no menor de ocho ni mayor de diez cuando el delito comprometa la defensa, seguridad o soberanía nacionales.

776 **Proyecto de Ley N.º 02999/2013, art. 7.** ***Interceptación ilícita de datos informáticos.***- El que, intercepta de manera deliberada e ilegítima, datos informáticos en transmisiones no públicas, dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas, provenientes de un sistema informático que transporte dichos datos informáti-

mula recomendó (i) incluir los elementos *deliberada* e *ilegítimamente*, pero (ii) no circunscribió la norma que debería infringirse para la configuración de la circunstancia agravante prevista en su segundo párrafo.

- **Proyecto de Ley N.º 03105/2013,** presentado el 18 de diciembre de 2013 por la congresista Carmen Omonte Durand[777]. En este caso, (i) se recomendó eliminar el elemento *dirigidas a un sistema informático* y, a diferencia de los proyectos de ley antes mencionados, (ii) no sugirió incorporar los elementos *deliberada* e *ilegítimamente*.

8.5.4. Regulación actual

Para comprender los alcances del delito de interceptación de datos informáticos, es necesario realizar dos precisiones, las cuales giran en torno a los artículos 162 y 162-B CP:

En primer lugar, en octubre de 2013, con la publicación de la LDI, no solo se incorporó el delito de interceptación ilegal de datos informáticos, sino que también se modificó el delito de interferencia telefónica[778], añadiéndose las mismas circunstancias agravantes previstas para el nuevo tipo penal. Esta

---

cos, será reprimido con une pena privativa de libertad no menor de tres ni mayor de seis años.
La pena privativa de la libertad será no menor de ocho ni mayor de diez años cuando el delito comprometa la defensa, la seguridad o la soberanía nacional.
La pena privativa de libertad será no menor de ocho ni mayor de diez años cuando el delito comprometa la defensa, la seguridad o la soberanía nacional.

777 **Proyecto de Ley N.º 03105/2013, art. 7. *Interceptación de datos informáticos.-*** El que, a través de las tecnologías de la información o de la comunicación intercepta datos informáticos en transmisiones no públicas, originadas en un sistema informático o efectuado dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos, será reprimido con una pena privativa de libertad no menor de tres ni mayor de seis años.
La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con las normas de la materia.
La pena privativa de libertad será no menor de ocho ni mayor de diez cuando el delito comprometa la defensa, seguridad o soberanías nacionales.

778 La Ley N.º 30096 generó la siguiente modificación:

precisión es importante porque excluye las llamadas de voz del ámbito de protección del delito estudiado en este capítulo.

Una situación similar ocurrió en marzo de 2014, cuando la Ley N.° 30171 reformó el delito de interceptación ilegal de datos, extendiendo dichos cambios también al delito de interferencia telefónica[779].

Es importante precisar que, a diferencia del delito de interceptación ilegal de datos, la última modificación del delito de interferencia telefónica data del 27 de julio de 2015, cuando se publicó el Decreto Legislativo N.° 1182 o "Decreto Legislativo que regula el uso de los datos derivados de las telecomunicaciones para la identificación, localización y geolocalización de equipos de comunicación, en la lucha contra la delincuencia y el crimen organizado"[780].

779 **CP, art. 162.-** El que, indebidamente, interfiere o escucha una conversación telefónica o similar será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años.
Si el agente es funcionario público, la pena privativa de libertad será no menor de cuatro ni mayor de ocho años e inhabilitación conforme al artículo 36, incisos 1, 2 y 4.
La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con las normas de la materia.
La pena privativa de libertad será no menor de ocho ni mayor de diez años cuando el delito comprometa la defensa, la seguridad o la soberanía nacionales.
La Ley N.° 30 171 incorporó la siguiente modificación:
CP, art. 162.- El que, indebidamente, interfiere o escucha una conversación telefónica o similar, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años.
Si el agente es funcionario público, la pena privativa de libertad será no menor de cuatro ni mayor de ocho años e inhabilitación conforme al artículo 36, incisos 1, 2 y 4.
La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con la Ley 27806, Ley de Transparencia y Acceso a la Información Pública.
La pena privativa de libertad será no menor de ocho ni mayor de diez años, cuando el delito comprometa la defensa, seguridad o soberanía nacionales.
Si el agente comete el delito como integrante de una organización criminal, la pena se incrementa hasta en un tercio por encima del máximo legal previsto en los supuestos anteriores.

780 El Decreto Legislativo N.° 1182 incorporó la última modificación:
CP, art. 162 CP.- El que, indebidamente, interviene o interfiere o escucha una conversación telefónica o similar, será reprimido con pena privativa de libertad no menor de cinco ni mayor de diez años.

En segundo lugar, el 26 de setiembre de 2015, se incorporó al Código Penal peruano el artículo 162-B, denominado *interferencia de comunicaciones electrónicas, de mensajería instantánea y similares*[781]. *La exposición de motivos nos permite comprender que el objeto de protección serán las comunicaciones electrónicas y, en consecuencia, también estarán excluidas de los alcances del delito de interceptación ilegal de datos informáticos:*

> Si bien la Ley N.º 30096, Ley de Delitos Informáticos, define a los datos informáticos como toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función, esta definición no se ajusta a los actuales conceptos de las comunicaciones electrónicas, mensajería inmediata y similares, puesto que estas comunicaciones representan un servicio de transmisión que consiste en el transporte de datos a través

---

La pena privativa de libertad será no menor de diez ni mayor de quince años:
1. Cuando el agente tenga la condición de funcionario o servidor público, y se impondrá además la inhabilitación conforme al artículo 36, incisos 1, 2 y 4.
2. Cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con la Ley 27806, Ley de Transparencia y Acceso a la Información Pública.
3. Cuando el delito comprometa la defensa, seguridad o soberanía nacionales.

Si el agente comete el delito como integrante de una organización criminal, la pena se incrementa hasta en un tercio por encima del máximo legal previsto en los supuestos anteriores

781 El Decreto Legislativo N.º 1234 incorporó el delito de interferencia de comunicaciones electrónicas, de mensajería instantánea y similares:

CP, art. 162-B.- El que, indebidamente, interviene o interfiere comunicaciones electrónicas o de mensajería instantánea o similares, será reprimido con pena privativa de libertad no menor de cinco ni mayor de diez años.

La pena privativa de libertad será no menor de diez ni mayor de quince años, cuando:
1. El agente tenga la condición de funcionario o servidor público, y se impondrá además la inhabilitación conforme al artículo 36, incisos 1, 2 y 4.
2. El delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con la Ley N.º 27806, Ley de Transparencia y Acceso a la Información Pública.
3. El delito comprometa la defensa, seguridad o soberanía nacionales.

Si el agente comete el delito como integrante de una organización criminal, la pena se incrementa hasta en un tercio por encima del máximo legal previsto en los supuestos anteriores.

> de redes de comunicaciones electrónicas, con inclusión de servicios de telecomunicaciones y servicios de transmisión en las redes utilizadas para la radiodifusión; en tanto, que los datos informáticos se definen como todo concepto, cifras o instrucciones que se tienen aisladas entre sí, sin seguir una organización o un orden específico, siendo entonces el concepto de dato aislado, o bien un conjunto de datos, que por su cuenta constituyen simples datos, pero que requieren de un ordenamiento, que es justamente un proceso.
>
> Realizada esta tarea, es decir, organizados los datos, estos ya no son solo símbolos, sino que son una información que puede ser leída, interpretada y compartida, siendo entonces diferente este término al de su unidad, pese a que actualmente se utilizan erróneamente en forma ambigua.
>
> Un ejemplo de comunicación electrónica es el utilizar el internet para enviar correos (*e-mail*), estos correos al ser transferidos se transforman en paquetes de datos (datos informáticos), los cuales viajan a través de una comunicación electrónica para que puedan llegar a su destino.
>
> [...] Así tenemos, por ejemplo, que las organizaciones criminales (bandas) que operan en el país se valen de medios para vulnerar las comunicaciones por medios electrónicos, tales como el Facebook y el WhatsApp para obtener la información personal, así como patrimonial de sus potenciales objetivos (ciudadanos), que les permita llevar a cabo sus acciones delictivas (extorsión, sicariato, sabotaje, pornografía infantil, entre otros).

Como el lector puede advertir, los artículos 162 y 162-B CP se erigen como normas de exclusión o delimitación del objeto de protección del delito de interceptación ilegal de datos informáticos, pues si bien estos comprenden tanto las llamadas por medios digitales[782] como los correos electrónicos o los servicios de mensajería instantánea -que, en estricto, son datos informáticos-, cuando la interferencia se refiera a estos, serán subsumidos en las dos normas previamente mencionadas:

782 Las llamadas telefónicas convencionales o analógicas no son una manifestación del envío de datos informáticos, al ser señales eléctricas transmitidas a través de líneas telefónicas. En cambio, las llamadas por VoIP, celulares o aplicaciones sí lo son al codificar, procesar y transmitir datos por medio de sistemas informáticos. El artículo 162 comprenderá ambos tipos de llamadas.

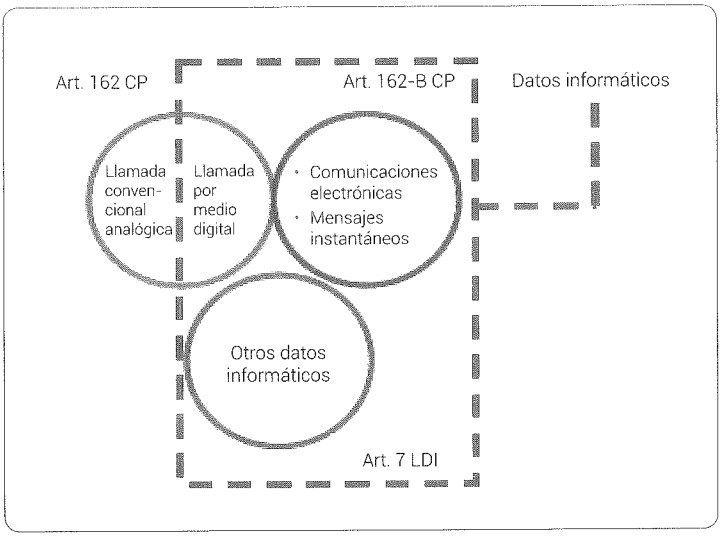


Diagrama 18. Relación de los delitos de interferencia telefónica (art. 162 CP), interferencia de comunicaciones electrónicas (art. 162-B CP) e interceptación ilegal de datos informáticos (art. 7 LDI). Elaboración propia.

Si analizamos las consecuencias jurídicas del delito, podemos advertir que el ordenamiento peruano sanciona con mayor intensidad los delitos que comprometen las comunicaciones telefónicas y electrónicas, en tanto se afectan los datos de contenido o la comunicación misma.

	Interferencia telefónica	Interferencia de comunicaciones electrónicas, de mensajería instantánea y similares	Interceptación de datos informáticos
	Art. 162 CP	Art. 162-B CP	Art. 7 LDI
Tipo base	5 a 10 años		3 a 6 años
El agente tiene la condición de agente o servidor público.	10 a 15 años, más inhabilitación		-
El delito recae sobre información secreta, reservada o confidencial	10 a 15 años		5 a 8 años
El delito compromete la defensa, seguridad o soberanía nacionales	10 a 15 años		8 a 10 años
Como parte de una organización criminal	Pena se incrementa en un tercio por encima del máximo legal		

Cuadro 28. Comparación de la sanción prevista en los delitos de interferencia telefónica, interferencia de comunicaciones electrónicas e interceptación de datos informáticos. Elaboración propia.

Dicho esto, centremos nuevamente nuestra atención en el delito de interceptación de datos informáticos y comparemos la redacción original con su versión vigente:

Art. 7 LDI (original)	Art. 7 LDI (actual)
Ley N.° 30096	**Modificado por la Ley N.° 30171**
El que, a través de las tecnologías de la información o de la comunicación, intercepta datos informáticos en transmisiones no públicas, dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años.	El que deliberada e ilegítimamente intercepta datos informáticos en transmisiones no públicas, dirigidos a un sistema informático, originados en un sistema informático o efectuado dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos, será reprimido con una pena privativa de libertad no menor de tres ni mayor de seis años.
La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con las normas de la materia.	La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con el TUO de la Ley 27806, Ley de Transparencia y Acceso a la Información Pública.
La pena privativa de libertad será no menor de ocho ni mayor de diez años cuando el delito comprometa la defensa, la seguridad o la soberanía nacionales.	La pena privativa de libertad será no menor de ocho ni mayor de diez cuando el delito comprometa la defensa, seguridad o soberanía nacionales. Si el agente comete el delito como integrante de una organización criminal, la pena se incrementa hasta en un tercio por encima del máximo legal previsto en los supuestos anteriores.

Cuadro 29. Regulación del delito de interceptación ilegal de datos informáticos, 2013-2024. Elaboración propia.

La actual tipificación del delito de interceptación ilícita de datos en la legislación penal peruana puede ser graficada de la siguiente forma:

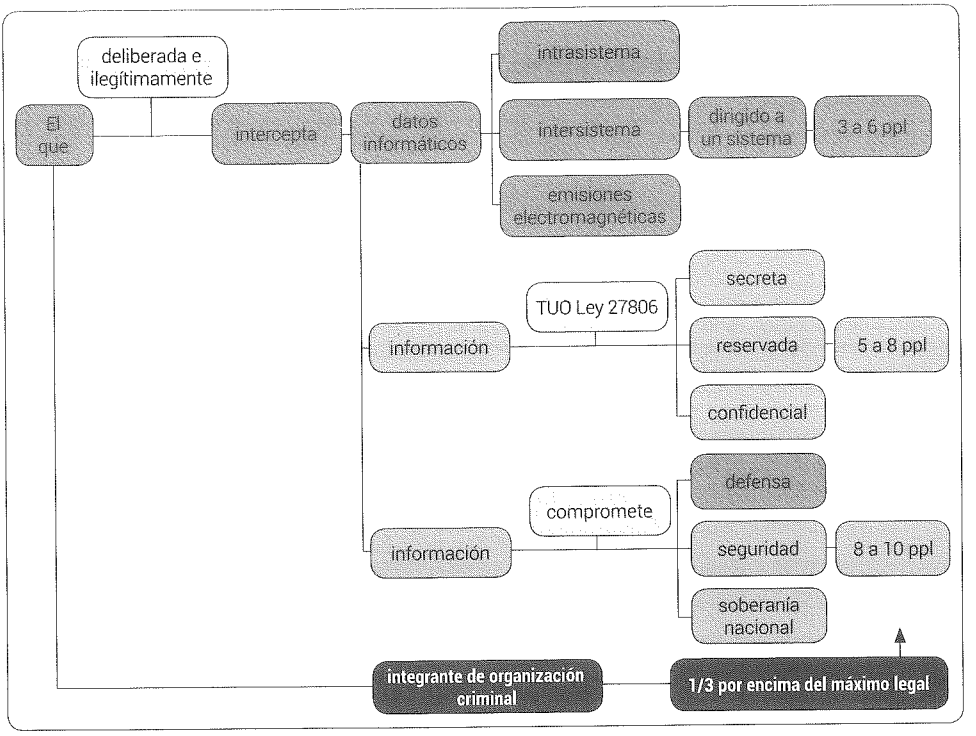


Diagrama 19. Estructura actual del delito de interceptación ilegal de datos informáticos en el sistema penal peruano. Elaboración propia.

Antes de continuar, es importante resaltar que el artículo 7 LDI recoge el *nomen iuris interceptación de datos informáticos*; mientras que el artículo 3 del Convenio utiliza una denominación mucho más precisa: *interceptación ilícita*. En una eventual modificación legislativa, se recomienda emplear el mismo *nomen iuris* para evitar confusiones terminológicas.

8.6. EL BIEN JURÍDICO PENALMENTE PROTEGIDO

Cierto sector de la doctrina considera que el bien jurídico protegido es "la privacidad, intimidad y el secreto de las comunicaciones"[783]; sin embargo, no considero adecuado asumir esta posición, ya que se protege la confidencialidad

783 Espinoza Calderón, *Delitos informáticos y nuevas modalidades delictivas*, cit., p. 90. En la misma línea: Arévalo Minchola/Vega Aguilar, *Ciberdelitos. Análisis en el sistema penal*, cit., p. 329; Pérez López, *Delitos regulados en leyes penales especiales*, cit., p. 147.

de los datos y de los sistemas, independientemente del tipo de contenido de la información transmitida.

La ubicación de este delito en la LDI genera problemas para la identificación del bien jurídico protegido. Por eso hay quienes sostienen que se protege tanto el derecho al secreto de las comunicaciones como la integridad, disponibilidad y confidencialidad de los datos y sistemas informáticos, siguiendo el modelo del Convenio de Budapest[784].

Una posición mucho más adecuada es la desarrollada por Oré Sosa, para quien "el objeto de protección es la[785] privacidad de las comunicaciones, en especial de la transmisión de datos informáticos".

Como ya se ha sostenido en esta obra, los términos confidencialidad (*confidentiality*), integridad (*integrity*) y disponibilidad (*availability*) son ampliamente conocidos en ciberseguridad[786] como la triada CIA, por sus siglas en inglés, y son los que nos permitirán identificar el bien jurídico penalmente protegido en este delito.

La importancia de estos conceptos se refleja en el Decreto Legislativo N.º 1412 o Ley de Gobierno Digital, pues establece en su artículo 31 que "el Marco de Seguridad Digital del Estado Peruano se constituye en el conjunto de principios, modelos, políticas, normas, procesos, roles, tecnología y estándares mínimos que permitan preservar la *confidencialidad, integridad, disponibilidad* de la información en el entorno digital administrado por las entidades de la Administración Pública".

---

784 Jiménez Herrera, *Manual de derecho penal informático*, cit., pp. 443 y s.

785 Oré Sosa, *Delictum. Apuntes de derecho penal*, cit., p. 204.

786 Recordemos que, en el glosario del Código de Derecho a la Ciberseguridad de España, actualizado al 31 de marzo del 2022, se define la *disponibilidad* de la siguiente manera: "Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren". La *integridad* es definida del siguiente modo: "Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada". Finalmente, la *confidencialidad* se define así: "Propiedad o característica consistente en que la información ni se pone a disposición, ni se releva a individuos, entidades o procesos no autorizados".

Esto no significa que cada delito deba proteger simultáneamente estos tres elementos, pues dependerá de la fórmula legislativa que ha recogido cada país para identificar su objeto de protección. Así, en el caso peruano, mientras el delito de acceso ilícito y la interceptación ilícita protegen la *confidencialidad*, los delitos de atentados contra datos y sistemas informáticos protegen la *integridad* y la *disponibilidad*.

Es importante resaltar que existe un problema en la ubicación o sistematización de este delito. El legislador peruano incorporó a la LDI un capítulo denominado *Delitos informáticos contra la intimidad y el secreto de las comunicaciones* [787] en el que lo ubicó junto al delito de tráfico ilegal de datos (art. 6 LDI). Sin embargo, este último delito fue reubicado, ya que retornó al Código Penal, ubicándose en el capítulo *Violación de la intimidad*, bajo el nombre de *tráfico ilegal de datos personales* (art. 154-A CP). La regulación actual impacta en la interpretación del bien jurídico protegido del delito analizado, pues pareciese que protege el derecho a la intimidad y a la inviolabilidad del secreto de las comunicaciones, previstos en los artículos 2.7 y 2.10 de nuestra Constitución Política.

Mi posición -la *confidencialidad* como bien jurídico protegido- se ve fortalecida por la tipificación de la interceptación de comunicaciones telefónicas (art. 162 CP) y electrónicas (art. 162-B CP), ya que, como he señalado, estas constituyen manifestaciones de los datos informáticos. No obstante, es posible advertir una diferencia sustancial: en estos casos, lo que se protege es el contenido mismo del mensaje transmitido, lo cual explica que el legislador peruano haya decidido ubicar estas conductas en el capítulo IV del título IV de la Parte Especial referido a la "Violación del secreto de las comunicaciones" dentro del Código Penal y no en la Ley de Delitos Informáticos.

Una eventual reforma legislativa debiese seguir la fórmula del Convenio de Budapest, esto es, ubicarlo bajo un mismo capítulo que tutele tanto la *confidencialidad*, *integridad* y *disponibilidad* de los datos y sistemas informáticos.

787 El nombre de este capítulo fue propuesto en el proyecto de Ley N.º 34-2011. En él se agruparon los siguientes delitos: **art. 8.-** Violación de la intimidad de la data personal; **art. 9.-** Violación del secreto de las comunicaciones; **art. 10.-** Revelación indebida de data o información de carácter personal. Como se puede apreciar, solo los dos primeros fueron aprobados.

8.7. TIPICIDAD OBJETIVA

Cuando el artículo 7 LDI se publicó, en octubre de 2013, incluyó el medio por el cual se realiza la interceptación: a través de las tecnologías de la información o de la comunicación. Sin embargo, en la modificación se eliminó este elemento típico, alejándonos de la propuesta del Convenio de Budapest -esto es, que el delito se cometa por medios técnicos-.

Al analizar la legislación comparada, se observa que Paraguay incluye el elemento *utilizando medios técnicos*, al igual que Chile. En el caso español se utiliza una fórmula similar: *mediante la utilización de artificios o instrumentos técnicos*[788]. En una eventual modificación se recomienda incluir esta expresión para precisar el medio que se emplea para la interceptación ilícita.

8.7.1. Sujetos

Si bien la doctrina nacional reconoce que estamos frente a un delito común, en tanto no se exige una condición especial en el **sujeto activo**, se sostiene que este delito es mayormente conocido por *phreakers*, es decir, "aquellos individuos que orientan sus estudios y ocio hacia el aprendizaje y comprensión del funcionamiento de teléfonos de diversa índole, tecnologías de telecomunicaciones, funcionamiento de compañías telefónicas, sistemas que componen una red telefónica y, por último, electrónica aplicada a sistemas telefónicos, vale decir, es el especialista en telefonía"[789].

Sobre este punto, debo precisar que este delito puede ser cometido por cualquier persona, ya que no exige una condición o conocimiento especial. Como se ha explicado en los capítulos anteriores, hoy en día no se necesita contar con conocimientos avanzados para cometer este tipo de delitos. Recordarlo evitará que al investigar estos casos incurramos en sesgos o prejuicios.

788 "En relación con la expresión mediante la utilización de artificios o instrumentos el Informe previo a la Convención de Budapest pone los siguientes ejemplos: los dispositivos que se conectan a las líneas de transmisión, los dispositivos que pueden utilizarse para obtener y grabar las comunicaciones inalámbricas, el uso de software, contraseñas y códigos" (Gil Gil y Hernández Berlinches, *Cibercriminalidad,* cit., pp. 208 y s.).

789 Jiménez Herrera, *Manual de derecho penal informático*, cit., p. 446.

Como bien indica Posada Maya, "[e]l sujeto activo también puede ser el titular legítimo de los datos que se trasmiten o alguna de las partes de una comunicación, cuando intercepta datos cuya transmisión depende de terceros. Esto es así, pues los delitos informáticos no solo protegen la intimidad personal o el derecho a las propias comunicaciones privadas, sino también la seguridad colectiva de las funciones y los sistemas informáticos"[790].

En este caso, el **sujeto pasivo** será el titular del bien jurídico afectado, pudiendo ser tanto una persona natural como una jurídica. En esta línea se afirma:

> Se trata de un tipo penal común. La ley tiende a configurar este delito a partir de un concepto unitario de víctima o de sujeto pasivo, de manera que además del titular de la seguridad de la información y los usuarios (Ley 1266 de 2008), se agrupan a los titulares de los datos violados en los sistemas informáticos interceptados o de las emisiones electromagnéticas que provengan de los sistemas que transportan datos (por ejemplo, las ondas de telefonía celular son ondas de ultra alta frecuencia [UHF] de 300 MHZ a 3 GHZ). Es necesario señalar que el sujeto pasivo puede ser una persona natural o una persona jurídica de derecho público o privado[791].

8.7.2. Acciones típicas

8.7.2.1. Interceptar

Es importante recordar que los artículos 162 y 162-B del Código Penal sancionan la interferencia telefónica y de comunicaciones electrónicas empleando dos verbos rectores: *intervenir* e *interferir*. El delito analizado en este capítulo no utiliza ninguno de esos verbos, por el contrario, utiliza el verbo *interceptar*. Pese a ello, dichos verbos son importantes para definir el alcance del verbo bajo análisis:

790 Posada Maya, *Los cibercrímenes: Un nuevo paradigma de criminalidad. Un estudio del título VII bis del Código Penal colombiano*, cit., p. 275.

791 *Ibid.*, p. 276.

	Interferencia telefónica	Interferencia de comunicaciones electrónicas (...)	Interceptación de datos informáticos
Intervenir	Sí	Sí	No
Interferir	Sí	Sí	No
Interceptar	No	No	Sí

Cuadro 30. Diferencia de verbos rectores de los delitos previstos en los artículos 162, 162-B CP y 7 LDI.

Considero que mientras que la interferencia de comunicaciones telefónicas o electrónicas puede permitir el acceso inmediato al contenido de mensajes orales, escritos o visuales, la interceptación de datos informáticos se centra en la captura de información digital en tránsito, a través de medios técnicos, sin necesidad de alterar el canal de comunicación.

Ahora bien, para la doctrina local, *interceptar* es "aprehender, captar y tener acceso a la comunicación que se transmite por medio de las tecnologías de la información y de la comunicación. Dicha comunicación no está dirigida para el sujeto activo; sin embargo, este, sabiendo por el medio que se transmite dicha comunicación, realiza un acceso ilícito y toma conocimiento del contenido de una comunicación no dirigida a su persona"[792]. En la misma línea, se sostiene que "la interceptación de datos informáticos se podría definir como la neutralización o interferencia del normal tráfico de información y de transmisión de datos que tiene lugar dentro de una determinada base o sistema informático, o en una parte de la misma; la misma que se realiza de manera no permitida, no autorizada o contraria al derecho"[793].

Miró Llinares, citado por Oré Sosa, define interceptar como "la captación de la transmisión o de la emisión electromagnética, de modo que el autor se asegure el dominio sobre los datos informáticos contenidos en la transmisión o en la emisión"[794]. Me adhiero a esta definición, pero con la precisión efectuada al inicio de este acápite.

[Caso 108] Un ejemplo de interceptación ilegal es un *ataque de intermediario*, también conocido como ataque *man-in-the-middle*, pues le permite al

792 Espinoza Calderón, *Delitos informáticos y nuevas modalidades delictivas*, cit., pp. 91 y s.

793 Arévalo Minchola/Vega Aguilar, *Ciberdelitos. Análisis en el sistema penal*, cit., p. 330;

794 Oré Sosa, *Delictum. Apuntes de derecho penal*, cit., p. 204.

agente espiar el circuito de comunicaciones entre el remitente y el receptor, haciéndose pasar por uno de ellos o ambos, comunicándose en su nombre.

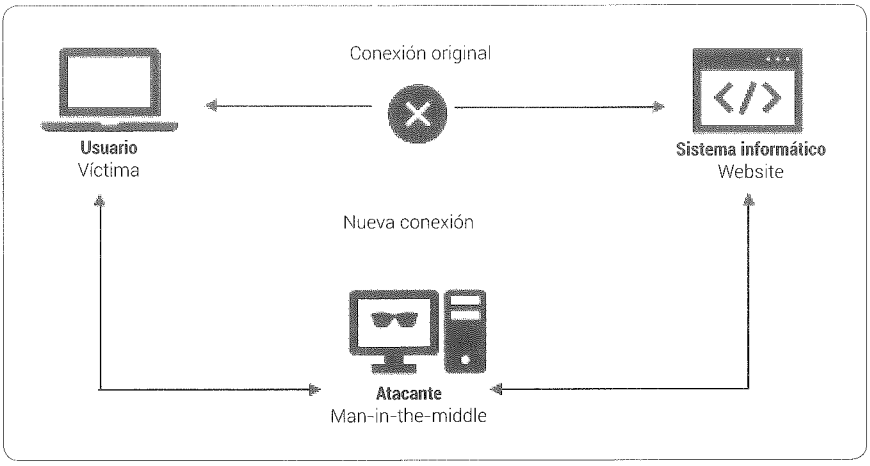


Diagrama 20. ¿Cómo funciona un ataque de intermediario?[795]

[Caso 109] En el 2021, el Equipo de Repuesta de Incidentes de Seguridad Digital advirtió la existencia de una variante del troyano de acceso remoto (RAT) que afecta dispositivos Android y sistemas operativos Windows, denominado LodaRAT. Este troyano tiene capacidades avanzadas como el robo de credenciales y, lo que nos interesa en este capítulo, espionaje de usuarios.

La campaña de distribución se realiza a través de correos electrónicos de *phishing* que contienen archivos adjuntos maliciosos, suplantando la identidad de instituciones financieras. En aquella época, se distribuían dos versiones del *malware* Loda4Android y Loda4Windows. El *malware* en referencia tiene la capacidad de leer e interceptar mensajes de texto (SMS) enviados o recibidos por la víctima[796].

795 Adaptado de Panda Media Center. *¿Qué es un ataque Man-in-the-Middle (MITM)? Definición y prevención*. Publicado el 13 de abril de 2022. https://www.pandasecurity.com/es/mediacenter/ataque-man-in-the-middle/

796 Centro Nacional de Seguridad Digital. *Alerta integrada de seguridad digital* N.º 34-2021. Lima: 13 de febrero de 2021, pp. 3 y 8. https://www.gob.pe/institucion/

Toda vez que el *malware* intercepta mensajes de textos, este ejemplo grafica un caso de interferencia de comunicaciones electrónicas -pese a que, en estricto, los mensajes son datos informáticos-.

8.7.3. Objeto del delito: datos informáticos y emisiones electromagnéticas

El objeto material de este delito viene dado tanto por los datos informáticos como por las emisiones electromagnéticas. Se protege la interceptación de dichas emisiones, en tanto, a partir de estas es posible reconstruir los datos informáticos.

8.7.3.1. En transmisiones no públicas

Son aquellas transmisiones privadas o restringidas cuyo contenido, incluso, puede ser de conocimiento público, pero que las partes de la comunicación no desean revelar, sino mantener de forma confidencial. Como se señala en el Informe Explicativo del Convenio de Budapest, la expresión *no pública* no excluye *per se* las comunicaciones que se realizan a través de redes públicas. En el mismo instrumento se explica que las partes involucradas podrían establecer que la información o servicio no sea accesible hasta que se efectúe determinado pago, por ejemplo, la televisión *pay per view*.

Algunos ejemplos permitirán comprender mejor este concepto:

- Transmisión de datos entre una computadora y determinado sistema previa autenticación.
- Conexión de un cajero automático con el servidor del banco.
- Transmisión de datos biométricos entre una aplicación de reconocimiento facial y un servidor informático.
- Acceso remoto de un empleado a su escritorio de trabajo (*remote desktop*).
- Envío o intercambio de archivos a través de enlaces restringidos de Google Drive o Dropbox.

pcm/informes-publicaciones/1683562-alerta-integrada-de-seguridad-digital-n-034-2021-pecert

- Datos médicos transmitidos entre una aplicación de salud y el sistema informático de la clínica o centro médico que lo administra.
- Conexión entre un sistema de videovigilancia y el servidor alojado en la nube.
- Sincronización de una billetera de criptomonedas con un determinado nodo de red.
- Transmisión de un pedido solicitado a través de un aplicativo y el sistema informático del restaurante.

Como el lector habrá advertido, la información transmitida no necesariamente será de naturaleza personal. Esto ha llevado a algunos autores a indicar que se protegen también "datos transmitidos de naturaleza impersonal, como aquellos referidos a las cosas que las personas compran en establecimientos de comercio, los metadatos u otra información residual de actividades privadas (conductas como la obtención de datos basura o *trashing*), los inventarios comerciales de las empresas, etcétera"[797].

Es importante recordar que la intervención de las llamadas telefónicas y de las comunicaciones electrónicas se encuentran previstas en los artículos 162 y 162-B CP, por lo que el artículo 7 LDI se ocupará de la transmisión del resto de datos informáticos.

8.7.3.2. Origen de las transmisiones

La legislación peruana sigue la fórmula propuesta en el Convenio de Budapest, esto es, establece que la transmisión de datos informáticos puede darse en tres ámbitos: dirigidos a un sistema informático, originados en un sistema informático o efectuados dentro del mismo sistema informático. El Informe Explicativo grafica este punto de la siguiente forma:

> 55. La comunicación en la forma de transmisión de datos informáticos puede tener lugar dentro de un único sistema informático (por ej., pasando del CPU a la pantalla o a la impresora), entre dos sistemas informáticos que pertenecen a una misma persona, entre dos ordenadores

797 Posada Maya, *Los cibercrímenes: Un nuevo paradigma de criminalidad. Un estudio del título VII bis del Código Penal colombiano*, cit., p. 279.

> que se comunican entre sí, o entre un ordenador y una persona (por ej., a través del teclado). No obstante, las Partes podrán exigir como elemento adicional que la comunicación sea transmitida entre sistemas informáticos que estén conectados de forma remota.

El Informe Explicativo fue aprobado hace poco más de dos décadas y, desde entonces, varios aspectos han cambiado o evolucionado. Por ejemplo, al describir un sistema informático, en dicho informe se menciona que la información pasa del CPU a la pantalla o a la impresora. Sin embargo, hoy en día, las impresoras funcionan como sistemas informáticos autónomos, capaces de imprimir documentos directamente desde la nube, sin necesidad de estar conectadas a una computadora. Años atrás, esto no era posible: las impresoras de matriz de puntos requerían una conexión física con una computadora para poder imprimir. En ese contexto, tenía sentido considerarlas parte de un único sistema informático.

A continuación, detallaré algunos ejemplos que permiten comprender los tres supuestos previstos en el artículo 7 LDI, en concordancia con el artículo 3 del Convenio de Budapest:

Datos dirigidos a un sistema informático:

- Colocar la contraseña en la página web de un banco.
- *Loguearse* a través del registro biométrico (rostro o huella) para ingresar a una aplicación.
- Utilizar un celular para abrir las puertas de un automóvil que cuente con sistemas informáticos.
- Subir documentos a la plataforma del Poder Judicial o del Ministerio Público.

Datos originados en un sistema informático:

- Alerta de seguridad enviadas por el sistema de videovigilancia del hogar o del trabajo al celular del usuario.
- Resultados de un examen que es realizado a través de la plataforma de la universidad y que, al finalizar, automáticamente envía la nota al estudiante.
- Información enviada por el POS de un restaurante.

- Dron que recolecta datos meteorológicos y los envía a una estación agrícola.

Datos efectuados dentro del mismo sistema informático:

- Información que pasa entre las capas internas del sistema como autenticación, verificación o ejecución de una aplicación y que no cuenta con conexión externa.
- Datos que se transfieren entre el CPU y la memoria RAM de la computadora.
- Intercambio de datos en una red domótica del hogar (temperatura, luz, movimiento) que operan en LAN.
- Comunicación entre dos máquinas virtuales que corren en el mismo servidor físico.

[Caso 110] A fines del 2024, la Policía Federal australiana arrestó a un hombre que habría instalado redes wifi gratuitas[798] en tres aeropuertos y vuelos locales. Las víctimas identificaban la red, la cual las redirigía a páginas simuladoras. Para *loguearse*, se solicitaba que abrieran sesión en su correo electrónico o red social para que el ciberdelincuente pudiese acceder a sus datos informáticos: usuario y contraseña, entre otros[799].

En este caso, el atacante espera obtener los datos de la víctima, los cuales se originan en un sistema informático (celular, *laptop* o *tablet*, por ejemplo). Para ello, creó una red de wifi falsa, pues, de este modo, interceptará los datos

798 Este tipo de puntos de conexión se conocen como "Hotspot. Es un lugar donde se puede acceder a una red *wireless* pública, ya sea gratuita o de pago. Pueden estar cibercafés, aeropuertos, centros de convenciones, hoteles y otros lugares de encuentro, para proporcionar acceso a su red o a Internet a los visitantes o invitados" (Angulo Aguirre, Luis. *Hacking & cracking – Redes inalámbricas Wi-Fi*, cit., p. 230).

799 Centro Nacional de Seguridad Digital. *Alerta integrada de seguridad digital N.º 262-2024*. Lima: 13 de noviembre de 2024, p. 4. https://www.gob.pe/institucion/pcm/informes-publicaciones/6183321-alerta-integrada-de-seguridad-digital-n-262-2024-cnsd. En el mismo sentido: "Cuidado con el WiFi de los aviones: hay estafadores que crean redes falsas en los vuelos", en *Xakata*, 28 de julio de 2024. https://www.xataka.com/seguridad/cuidado-wifi-aviones-policia-detiene-a-estafadores-que-crean-redes-falsas-vuelos

informáticos de la víctima -quien no tiene conocimiento ni ha brindado su autorización para que la información en tránsito sea recopilada-.

8.7.3.3. Emisiones electromagnéticas

Como se aclara en el Informe Explicativo del Convenio de Budapest, las emisiones electromagnéticas no constituyen en sí mismas datos informáticos ni se equiparan a ellos. Sin embargo, su protección se justifica en la medida en que, mediante su captación, es posible acceder a datos informáticos contenidos o transmitidos por un sistema.

[Caso 111] El *Van Eck phreaking* o *radiación Van Eck* es un tipo de ataque de espionaje en el que se intercepta y analiza la radiación electromagnética (radiofrecuencia) emitida por los dispositivos informáticos. Con esta captura, los ciberdelincuentes pueden reconstruir y extraer información sensible sin tener acceso físico. De este modo, se puede obtener información como texto o imágenes mostradas en una pantalla o, incluso, las pulsaciones de teclas ingresadas[800].

Este ataque fue identificado en 1985 por el científico Wim Van Eck, quien utilizó un televisor y un equipo valorizado en 15 dólares. Si bien los dispositivos actuales son mucho más sofisticados, este tipo de ataque aún es posible, pero el ciberdelincuente tendría que invertir alrededor de 2000 dólares y ubicarse en un radio cercano al sistema objetivo -lo que, en la práctica, generaría demasiadas contingencias y riesgos-.

[Caso 112] En el 2016, el FBI alertó sobre dispositivos como el KeySweeper, un cargador USB que escondía *keyloggers*: el atacante registraba las pulsaciones de los teclados inalámbricos[801].

800 "Everything you need to know about Van Eck Phreaking", en *Liberty Center One*, 28 de julio de 2020. https://www.libertycenterone.com/blog/van-eck-phreaking/
VPN UNLIMITED. *Van Eck Phreaking*, https://www.vpnunlimited.com/es/help/cybersecurity/van-eck-phreaking

801 ESET. *El FBI advirtió sobre cargadores USB que esconden keyloggers*, publicado el 24 de mayo de 2016. https://www.welivesecurity.com/la-es/2016/05/24/fbi-advirtio-cargadores-usb-keyloggers/

El funcionamiento de este *keylogger* es el siguiente: el usuario conecta el cargador a un enchufe y este empieza a buscar teclados inalámbricos de Microsoft que no funcionen con Bluetooth, que se ubiquen en una banda de 2.4 GHz y que hayan sido lanzados antes del 2011. Dicho esto, vulnera la transmisión inalámbrica del teclado. Según los investigadores de ESET, las funciones de este dispositivo podrían ampliarse peligrosamente[802].



Imagen 27. Anuncio publicado por el FBI en el que se alertaba sobre el uso del *keylogger*[803].

802 "Además de registrar y almacenar las pulsaciones del teclado, el keylogger puede ser mejorado con nuevas funcionalidades añadiéndole nuevos módulos o complementos. Esto permitiría, por ejemplo, enviar la información capturada a un atacante utilizando un chip GSM opcional, o almacenarlas en una memoria flash para enviarlas vía inalámbrica cuando el atacante se acerque a una distancia prudencial del dispositivo. De hecho, el atacante bien podría estar tranquilamente en su casa monitorizando la información robada del teclado con una herramienta que las fuera mostrando en tiempo real en una web o recibiendo mensajes SMS en su móvil cada vez que la víctima pulsase alguna palabra o conjunto de palabras clave como www.mibanco.com" (ESET. *KeySweeper: grabando las pulsaciones de tu teclado por 10 dólares*, publicado el 16 de junio de 2015. https://www.welivesecurity.com/la-es/2015/01/16/keysweeper-grabando-pulsaciones-teclado/).

803 "Beware of fake USB chargers that wirelessly record everything you type, FBI warns", en *The Hacker News*, 24 de mayo de 2016. https://thehackernews.com/2016/05/usb-charger-keylogger.html

8.7.4. Circunstancias agravantes específicas

8.7.4.1. Por el tipo de información

La primera circunstancia agravante se configura por el tipo de contenido interceptado. Así, debemos acudir al ordenamiento extrapenal para precisar los alcances del segundo párrafo del artículo 7 LDI, pues sanciona con pena privativa de libertad no menor de cinco ni mayor de ocho cuando el delito recae sobre información clasificada como secreta, reservada o confidencial de conformidad con el TUO de la Ley N.° 27806.

El artículo 15 del TUO de la Ley N.° 27806 establece los supuestos específicos que calzan en la categoría **información secreta**, dividiéndolo en dos escenarios: información clasificada en el ámbito militar e información clasificada en el ámbito de la inteligencia, tanto externa como interna.

Información secreta	
Información clasificada, ámbito militar	**Información clasificada, ámbito de la inteligencia**
Planes de defensa militar contra posibles agresiones de otros Estados, logísticos, de reserva y movilización y de operaciones especiales, así como oficios y comunicaciones internas que hagan referencia expresa a los mismos.	Los planes estratégicos y de inteligencia, así como la información que ponga en riesgo sus fuentes.
Las operaciones y planes de inteligencia y contrainteligencia militar.	Los informes que, de hacerse públicos, perjudicarían la información de inteligencia.
Desarrollos técnicos y/o científicos propios de la defensa nacional.	Aquellos informes oficiales de inteligencia que, de hacerse públicos, incidirían negativamente en las excepciones contempladas en el inciso a) del numeral 2 del artículo 15 del TUO de la Ley 27806.
Órdenes de operaciones, logísticas y conexas, relacionadas con planes de defensa militar contra posibles agresiones de otros Estados o de fuerzas irregulares militarizadas internas y/o externas, así como de operaciones en apoyo a la Policía Nacional del Perú, planes de movilización y operaciones especiales relativas a ellas.	Información relacionada con el alistamiento del personal y material.
Planes de defensa de bases e instalaciones militares.	Las actividades y planes estratégicos de inteligencia y contrainteligencia, de los organismos conformantes del Sistema de Inteligencia Nacional, así como la información que ponga en riesgo sus fuentes.
El material bélico, sus componentes, accesorios, operatividad y/o ubicación cuyas características pondrían en riesgo los planes de defensa militar contra posibles agresiones de otros Estados o de fuerzas irregulares militarizadas internas y/o externas, así como de operación en apoyo a la Policía Nacional del Perú, planes de movilización y operaciones especiales relativas a ellas.	Información del personal civil o militar que desarrolla actividades de Seguridad Nacional y que pueda poner en riesgo la vida e integridad de las personas involucradas.
Información del Personal Militar que desarrolla actividades de Seguridad Nacional y que pueda poner en riesgo la vida e integridad de las personas involucradas.	La información de inteligencia que contemple alguno de los supuestos contenidos en el artículo 15 numeral 1 del TUO de la Ley 27806.

Cuadro 31. Información secreta, según el TUO de la Ley 27806. Elaboración propia.

De otro lado, la **información reservada** se encuentra regulada en el artículo 16 de la citada norma. Al igual que en el caso anterior, podemos dividirlo en dos supuestos, según afecte interna o externamente la seguridad nacional:

Información reservada	
Ámbito interno de la seguridad nacional	**Ámbito externo de la seguridad nacional**
Los planes de operaciones policiales y de inteligencia, así como aquellos destinados a combatir el terrorismo, tráfico ilícito de drogas y organizaciones criminales, así como los oficios, partes y comunicaciones que se refieran expresamente a ellos.	Elementos de las negociaciones internacionales que de revelarse perjudicarían los procesos negociadores o alteraran los acuerdos adoptados, no serán públicos por lo menos en el curso de las mismas.
Las informaciones que impidan el curso de las investigaciones en su etapa policial dentro de los límites de la ley, incluyendo los sistemas de recompensa, colaboración eficaz y protección de testigos, así como la interceptación de comunicaciones amparadas por la ley.	Información que al ser divulgada oficialmente por el Ministerio de Relaciones Exteriores pudiera afectar negativamente las relaciones diplomáticas con otros países.
Los planes de seguridad y defensa de instalaciones policiales, establecimientos penitenciarios, locales públicos y los de protección de dignatarios, así como los oficios, partes y comunicaciones que se refieran expresamente a ellos.	La información oficial referida al tratamiento en el frente externo de la información clasificada en el ámbito militar de acuerdo con lo señalado en el inciso a) del numeral 1 del artículo 15 del TUO de la Ley 27806.
El movimiento del personal que pudiera poner en riesgo la vida e integridad de las personas involucradas o afectar la seguridad ciudadana.	Los contratos de asesoría financiera o legal para realizar operaciones de endeudamiento público o administración de deuda del Gobierno Nacional; que de revelarse, perjudicarían o alterarían los mercados financieros, no serán públicos por lo menos hasta que se concreten las mismas.
El armamento y material logístico comprometido en operaciones especiales y planes de seguridad y defensa del orden interno.	
La información contenida en los Reportes de actividades con las sustancias químicas tóxicas y sus precursores listados en la Convención sobre la Prohibición del Desarrollo, la Producción, el Almacenamiento y el Empleo de Armas Químicas y sobre su Destrucción; la información contenida en los Reportes sobre las instalaciones de producción de las sustancias químicas orgánicas definidas; la información relacionada con las inspecciones nacionales e inspecciones realizadas por la Secretaría Técnica de la Organización para la Prohibición de las Armas Químicas; la información concerniente a los procesos productivos en donde intervienen sustancias químicas tóxicas y sus precursores de las Listas 1, 2 y 3 de dicha Convención; y la información concerniente al empleo de las sustancias químicas tóxicas y sus precursores de las Listas 1 y 2 de dicha Convención.	

Cuadro 32. Información reservada, según el TUO de la Ley N.° 27806. Elaboración propia.

Finalmente, los supuestos que integran la **información confidencial** se encuentran establecidos en el artículo 17 del TUO de la Ley N.° 27806.

Información confidencial
La información que contenga consejos, recomendaciones u opiniones producidas como parte del proceso deliberativo y consultivo previo a la toma de una decisión de gobierno, salvo que dicha información sea pública. Una vez tomada la decisión, esta excepción cesa si la entidad de la Administración Pública opta por hacer referencia en forma expresa a esos consejos, recomendaciones u opiniones.
La información protegida por el secreto bancario, tributario, comercial, industrial, tecnológico y bursátil que están regulados, unos por el inciso 5 del artículo 2 de la Constitución, y los demás por la legislación pertinente.
La información vinculada a investigaciones en trámite referidas al ejercicio de la potestad sancionadora de la Administración Pública, en cuyo caso la exclusión del acceso termina cuando la resolución que pone fin al procedimiento queda consentida o cuando transcurren más de seis (6) meses desde que se inició el procedimiento administrativo sancionador, sin que se haya dictado resolución final.
La información preparada u obtenida por asesores jurídicos o abogados de las entidades de la Administración Pública cuya publicidad pudiera revelar la estrategia a adoptarse en la tramitación o defensa en un proceso administrativo o judicial, o de cualquier tipo de información protegida por el secreto profesional que debe guardar el abogado respecto de su asesorado. Esta excepción termina al concluir el proceso.
La información referida a los datos personales cuya publicidad constituya una invasión de la intimidad personal y familiar. La información referida a la salud personal, se considera comprendida dentro de la intimidad personal. En este caso, sólo el juez puede ordenar la publicación sin perjuicio de lo establecido en el inciso 5 del artículo 2 de la Constitución Política del Estado. Por su parte, no opera la presente reserva cuando la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones requiera información respecto a los bienes e ingresos de los funcionarios públicos, o cuando requiera otra información pertinente para el cumplimiento de las funciones de la Unidad de Inteligencia Financiera del Perú - UIF-Perú.
Aquellas materias cuyo acceso esté expresamente exceptuado por la Constitución o por una Ley aprobada por el Congreso de la República.

Cuadro 33. Información confidencial, según el TUO de la Ley N.º 27806. Elaboración propia.

8.7.4.2. Por el riesgo que representa

El tercer párrafo del artículo 7 LDI sanciona con no menos de ocho ni más de diez años de pena privativa de libertad a quien comete este ilícito y compromete la defensa, la seguridad o la soberanía nacional.

[Caso 113] En el 2012, se descubrió que un gusano propalado a nivel mundial afectó a más de 55 mil ordenadores. El objetivo central de los atacantes fue sustraer información confidencial de agencias gubernamentales, laboratorios de energía nuclear, entidades del sector aeroespacial y militar de más de 39 países del Este de Europa, Asia Central y la antigua Unión Soviética. Este accionar también afectó instalaciones en Estados Unidos e Italia. Si bien el origen del ataque no fue aclarado, se baraja la posibilidad de que sean ciberdelincuentes localizados en Rusia o personal afín al gobierno de Corea del Norte[804].

804 Este caso se conoce como "Octubre Rojo" (Pérez-Prat Durbán, "Los ciberataques y el uso de la fuerza en las relaciones internacionales", cit., p. 29).

Por el tipo de información sustraída y las entidades atacadas, este ejemplo calza en el supuesto de compromiso de la defensa, la seguridad o la soberanía nacional. Por razones obvias, no se ha difundido qué información específica fue afectada. Este dato será importante para identificar en qué supuesto concretamente se subsumiría.

De otro lado, sería importante precisar la redacción de la agravante recogida en el tercer párrafo, pues actualmente indica cuando el delito comprometa la defensa, seguridad o soberanía nacionales. Al respecto, la expresión *el delito comprometa* es ambigua, por lo que sugiero utilizar una fórmula ya empleada en otros delitos como el de contaminación ambiental: *cause o pueda causar perjuicio*.

8.7.4.3. Por la condición del agente

La última circunstancia agravante prevista en el artículo 7 LDI está dada por la comisión del delito como parte de una organización criminal, en cuyo caso la pena se incrementa hasta en un tercio por encima del máximo legal previsto.

[Caso 114] Durante el primer gobierno de Donald Trump, los ataques atribuidos a la organización conocida como APT33 (Advanced Persistent Threat 33) adquirieron notoriedad en el ámbito de la seguridad informática a nivel mundial[805].

La firma de ciberseguridad FireEye concluyó que este grupo tenía capacidades destructivas y que, desde el 2013, se dedicaban al ciberespionaje. En este sentido, se sostiene que sus principales objetivos fueron empresas del sector de la aviación, militar, comercial y energético. Si bien el presidente Trump acusó a Irán de lanzar ciberataques contra la infraestructura crítica y el sistema financiero y militar de Estados Unidos, no ha mencionado al grupo APT33.

805 "APT33, el grupo de hackers iraní al que se atribuyen ataques a Estados Unidos, Arabia Saudita y Corea del Sur", en *BBC*, 16 de octubre de 2017. https://www.bbc.com/mundo/noticias-41637526

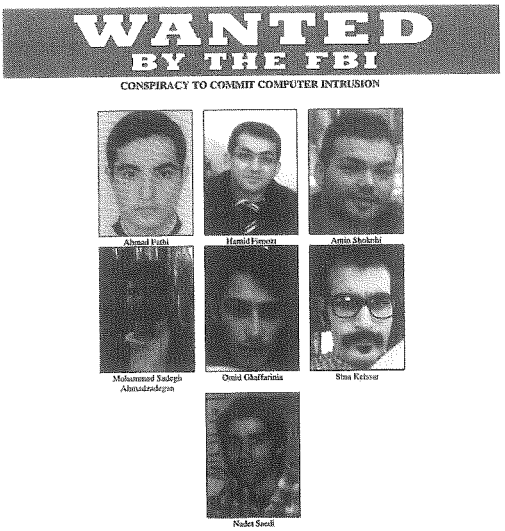


Imagen 28. Anuncio publicado por el FBI en el que se alertaba sobre siete ciudadanos implicados en diversos ciberataques[806].

8.8. TIPICIDAD SUBJETIVA

Desde el análisis de la tipicidad subjetiva, se debe precisar que esta conducta únicamente puede ser dolosa, descartando así las acciones culposas. Al igual que en otros delitos de esta ley, el legislador incluyó el término *deliberadamente*, razón por la cual, el dolo eventual es excluido.

8.9. LAS SITUACIONES DE JUSTIFICACIÓN EN EL DELITO DE INTERCEPTACIÓN ILÍCITA DE DATOS INFORMÁTICOS

Este delito también exige que la conducta sea ilegal, es decir, debe ser un hecho típico y antijurídico -o, en palabras de la Convención de las Naciones Unidas contras la Ciberdelincuencia, *sin derecho*-.

806 FBI. *Iranian DDoS Attacks*. https://thehackernews.com/2016/05/usb-charger-keylogger.html

Sobre el particular, Espinoza Calderón identificó un pronunciamiento de la Sala Penal de Apelaciones de Ayacucho en el que se concluye lógicamente que la ausencia de autorización del titular es imprescindible para la configuración del tipo penal:

> Para acceder a un soporte digital o electrónico que contenga información relacionada con datos personales protegidos por la ley de protección de los datos personales, como es la intimidad o privacidad, constitucionalmente protegidos, se requiere a falta de consentimiento del titular, autorización judicial; de lo contrario carecen de efecto legal alguno[807].

8.9.1. Registro remoto de equipos informáticos

Algunos ordenamientos, como el italiano, el francés y el español[808], facultan a las fuerzas del orden, con autorización judicial, a acceder a los datos informáticos transmitidos desde o hacia un sistema informático. Este acto de

807 Espinoza Calderón, *Delitos informáticos y nuevas modalidades delictivas*, cit., p. 92.

808 Recomiendo revisar el Capítulo IX, registro remoto sobre equipos informáticos, de la Ley de Enjuiciamiento Criminal de España para comprender los alcances de la medida bajo comentario:

Art. 588 *septies* a. Presupuestos

1. El juez competente podrá autorizar la utilización de datos de identificación y códigos, así como la instalación de un *software*, que permitan, de forma remota y telemática, el examen a distancia y sin conocimiento de su titular o usuario del contenido de un ordenador, dispositivo electrónico, sistema informático, instrumento de almacenamiento masivo de datos informáticos o base de datos, siempre que persiga la investigación de alguno de los siguientes delitos:
   a) Delitos cometidos en el seno de organizaciones criminales.
   b) Delitos de terrorismo.
   c) Delitos cometidos contra menores o personas con capacidad modificada judicialmente.
   d) Delitos contra la Constitución, de traición y relativos a la defensa nacional.
   e) Delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o la telecomunicación o servicio de comunicación.
2. La resolución judicial que autorice el registro deberá especificar:
   a) Los ordenadores, dispositivos electrónicos, sistemas informáticos o parte de los mismos, medios informáticos de almacenamiento de datos o bases de datos, datos u otros contenidos digitales objeto de la medida.

investigación es conocido como *registro remoto de equipos informáticos* y puede llevarse a cabo de dos formas:

> 1) accediendo a los datos a través de una red (*computer network*) que sea accesible a través del equipo que se ha localizado e intervenido físicamente, bien sea como consecuencia de una entrada y registro de otra manera. A su vez, el acceso remoto a datos desde un dispositivo intervenido físicamente puede realizarse mediante la instalación de *spyware*; y 2) mediante el acceso a los datos almacenados en equipos informáticos que no esté físicamente localizados o accesibles, pero a los cuales puede accederse mediante la utilización de programas espía o *spyware*, un *software* específico que permite "entrar" en el equipo, sin que, de ordinario, su usuario lo advierta. La primera medida suele denominarse *registro ampliado* o *extended search of computers*. El acceso remoto a datos desde un dispositivo intervenido físicamente, a los cuales se accede a su vez mediante *spyware* (y no a través de red), se suele denominar *online investigation light*. La segunda modalidad mencionada es la que se denomina *registro remoto* o *remote search of computers* y también *genuine on-line search*. Además, a través del registro remoto a través de *spyware*, se podría a su vez acceder a otros equipos que estuvieran conectados a la red del equipo "intervenido" o "hackeado". El registro ampliado y el registro remoto mediante instalación de *software* requieren un análisis diferenciado, pues, aunque el acceso al equipo informático se produce en ambos casos a distancia o de modo remoto,

---

b) El alcance de la misma, la forma en la que se procederá al acceso y aprehensión de los datos o archivos informáticos relevantes para la causa y el *software* mediante el que se ejecutará el control de la información.
c) Los agentes autorizados para la ejecución de la medida.
d) La autorización, en su caso, para la realización y conservación de copias de los datos informáticos.
e) Las medidas precisas para la preservación de la integridad de los datos almacenados, así como para la inaccesibilidad o supresión de dichos datos del sistema informático al que se ha tenido acceso.

3. Cuando los agentes que lleven a cabo el registro remoto tengan razones para creer que los datos buscados están almacenados en otro sistema informático o en una parte del mismo, pondrán este hecho en conocimiento del juez, quien podrá autorizar una ampliación de los términos del registro.

> la forma de acceso es diferente y su regulación también difiere en lo que se refiere a los presupuestos y a su ámbito de aplicación[809].

Toda vez que es una medida de intrusión muy severa[810], se exige una lista de delitos estipulados taxativamente y que se analice acuciosamente tanto la proporcionalidad (idoneidad, necesidad y proporcionalidad en sentido estricto) como su duración.

En los países que cuentan con regulación expresa, si la interceptación de datos informáticos es provocada por agentes policiales o fuerzas del orden debidamente autorizados por una decisión judicial, la conducta será típica, pero no ilegítima por cuanto no contravendría el ordenamiento jurídico.

En la legislación procesal penal peruana, esta figura no se encuentra prevista, por lo que, en virtud del principio de legalidad procesal, no podría emplearse. Al margen de las consecuencias penales que afrontaría el funcionario que ejecutara un registro remoto, la información obtenida sería excluida al ser prueba prohibida.

---

809 Bachmaier Winter, Lorena. "Registro remoto de equipos informáticos en la Ley Orgánica 13/2015: Algunas cuestiones sobre el principio de proporcionalidad". En: Cedeño Hernán, Marina. *Nuevas tecnologías y derechos fundamentales en el proceso.* Navarra: Thomson Reuters / Aranzadi, 2017, p. 87.

810 Algunos autores sostienen que es una de las medidas más invasivas que puede albergar el ordenamiento procesal y que, si bien aporta enorme utilidad, la dificultad que supone su puesta en funcionamiento limita su utilización: "En definitiva, es una medida que permite desde hacer una entrada y registro remota, hasta escuchar a los interlocutores de una llamada, visionar los mensajes que se intercambia una persona con terceros, inspeccionar el contenido completo de un dispositivo de almacenamiento masivo de información, activar los micrófonos y registrar todas las conversaciones que tenga una persona en el lugar en que esté con que tenga junto a si el dispositivo o incluso acceder al GPS del terminal móvil posicionando a un individuo en todo momento, o lo que es lo mismo, con una sola medida podríamos activar todas las que permite nuestro ordenamiento procesal" (Pillado Quintas, Víctor. "Las medidas de investigación tecnológica. Visión del ministerio fiscal". En: Pereira Puigvert, Sílvia y Francesc Ordóñez Ponz [dirs.]. *Investigación y proceso penal en el Siglo XXI, nuevas tecnologías y protección de datos.* Cizur Menor: Thomson Reuters / Aranzadi, 2021, p. 100).

8.10. CONSUMACIÓN

La doctrina local considera que nos encontramos frente a un delito de mera actividad y que, en consecuencia, no se admite la tentativa, ya que se consumaría con el simple cumplimiento del verbo rector *interceptar*[811].

De otro lado, Oré Sosa anota que "la conducta típica (interceptar) debe realizarse en pleno proceso de transmisión de los datos, proceso que concluye cuando el destinatario adquiere dominio sobre estos, la interceptación posterior a este momento dará lugar a la aplicación de otro tipo penal, como el de acceso ilícito"[812].

A diferencia de la doctrina mayoritaria, considero que este delito sí exige un resultado: la lesión del bien jurídico protegido seguridad informática o, de forma específica, la confidencialidad de los datos. De este modo, este ilícito no es un paso previo a la comisión de otros tantos como los ataques contra la integridad o disponibilidad de los datos o sistemas informáticos, sino que se erige como un tipo penal independiente que custodia la confidencialidad. En consecuencia, desde mi punto de vista, sí es posible sancionar la tentativa. La posición defendida en esta obra es compartida por Posada Maya:

> En el sentido del tipo penal estudiado, la interceptación de datos informáticos es un delito de resultado (in)material, que puede ser realizado por acción, mediante la manipulación (en sentido amplio) de cualquier clase de terminal pública o privada o sistema de comunicaciones, utilizando medios técnicos automatizados. Como puede observarse, estos delitos en realidad no son de mera conducta, pues exigen una modificación lógica o informática tangible sobre el cual recae la acción criminal, que no siempre tiene una manifestación tangible o material, perceptible en el mundo exterior. Se trata de una nueva perspectiva, una nueva estructura dogmática, que implica verificar la modificación

811 Arévalo Minchola/Vega Aguilar, *Ciberdelitos. Análisis en el sistema penal*, cit., p. 336. En la misma línea, Jiménez Herrera (*Manual de derecho penal informático*, cit., p. 454). También, Meneses Gonzáles/Meneses Ochoa, *La cibercriminalidad: Consideración criminológica, político-criminal, dogmática, procesal y cooperación internacional*, cit., p. 327.

812 Oré Sosa, *Delictum. Apuntes de derecho penal*, cit., p. 204 y s.

(in)material o lógica de objetos (como los datos informáticos o la información) sobre los cuales recae la acción cibercriminal[813].

8.11. CONCURSOS

Al igual que en los casos de acceso ilícito, la interceptación ilegal de datos informáticos no es un paso previo necesario para la comisión de atentados contra datos o sistemas informáticos; sin embargo, existirán supuestos en los que secuencialmente se produzcan. En esos casos, el caso se resolverá tomando en consideración que se trata de una sola unidad de hecho típico.

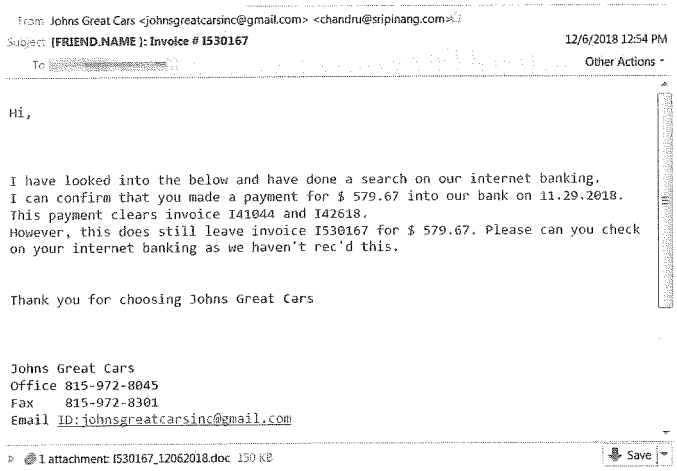
El uso de *spyware* es común en los casos de fraude informático, ya que los ciberdelincuentes emplean este tipo de *malware* no solo para dañar datos y sistemas, sino también para interceptar la información transmitida por el usuario afectado.

[Caso 115] EMOTET es un *malware* que inicialmente fue concebido como un troyano bancario, pero que actualmente es considerado uno polimórfico, es decir, cambia de forma cada cierto tiempo para realizar acciones maliciosas diversas: robo de información, *spam*, distribución de aplicaciones maliciosas, ataques de denegación de servicios, entre otras[814].

Su distribución se realizaba mediante archivos adjuntos a correos electrónicos enviados de forma masiva (*spam*). En el 2020, se descubrió que atacaba redes de wifi, escaneándolas en búsqueda de nuevos objetivos. Como se puede apreciar, sus diferentes funciones le permiten interceptar datos informáticos con la finalidad de cumplir los objetivos previstos por los ciberdelincuentes que dirigen el ataque.

813 Posada Maya, *Los cibercrímenes: Un nuevo paradigma de criminalidad. Un estudio del título VII bis del Código Penal colombiano*, cit., pp. 282 y s.

814 Incibe. *Emotet*, https://www.incibe.es/servicio-antibotnet/info/Emotet Kaspersky. *Emotet: La mejor manera de protegerte del troyano.* https://latam.kaspersky.com/resource-center/threats/emotet
Interpol. *World's most dangerous malware EMOTET disrupted through global action.* Disponible en:https://www.europol.europa.eu/media-press/newsroom/news/world's-most-dangerous-malware-emotet-disrupted-through-global-action


From: Johns Great Cars <johnsgreatcarsinc@gmail.com> <chandru@sripinang.com>
Subject: (FRIEND.NAME): Invoice # I530167 12/6/2018 12:54 PM
To: Other Actions

Hi,

I have looked into the below and have done a search on our internet banking.
I can confirm that you made a payment for $ 579.67 into our bank on 11.29.2018.
This payment clears invoice I41044 and I42618.
However, this does still leave invoice I530167 for $ 579.67. Please can you check on your internet banking as we haven't rec'd this.

Thank you for choosing Johns Great Cars

Johns Great Cars
Office 815-972-8045
Fax 815-972-8301
Email ID:johnsgreatcarsinc@gmail.com

1 attachment: I530167_12062018.doc 150 KB Save

Imagen 29. Correo electrónico empleado para la distribución del *malware* a través del archivo adjunto en formato de documento[815].

8.12. PENALIDAD

En este delito pueden identificarse cuatro tipos de variables. La modalidad básica sanciona la interceptación ilegal de datos con una pena privativa de libertad que oscila entre tres y seis años. Sin una justificación clara, el legislador omitió incluir los días multa, a diferencia de lo que hizo en los delitos de acceso ilícito y atentados contra la integridad de los datos y sistemas informáticos.

Ahora bien, aunque la pena establecida para este delito es compatible con la prevista para el acceso ilícito -pues ambas conductas afectan la confidencialidad de la información-, no ocurre lo mismo con los delitos de daños informáticos y sabotaje. Como se ha señalado, estos últimos generan un perjuicio considerablemente mayor, lo que plantea un problema de proporcionalidad en la aplicación de las sanciones.

En un segundo nivel, cuando el ilícito afecta información secreta, reservada o confidencial, la pena privativa de libertad fluctúa entre cinco y ocho años. Esta sanción resulta desproporcionada y excesiva en comparación con otros delitos que verdaderamente comprometen la seguridad informática y pueden

815 Sophos. *Emotet101, stage 1: The spam ire*, publicado el 5 de marzo de 2019. https://news.sophos.com/en-us/2019/03/05/emotet-101-stage-1-the-spam-lure/

generar daños de gran magnitud, como un ataque a los sistemas de una entidad financiera o la vulneración del secreto informático de una cadena de clínicas.

En un tercer y último nivel, se castiga con pena privativa de libertad no menor de ocho ni mayor de diez años cuando el delito compromete la defensa, seguridad o soberanía nacional. En este caso, la gravedad se encontraría justificada en tanto no solo se deberá acreditar la interceptación ilegal de datos, sino que, como consecuencia directa de esta, se han expuesto o comprometido tres pilares esenciales estatales.

Finalmente, con poco criterio técnico, se establece una circunstancia agravante adicional, por la condición del agente. Esto es, si el delito es cometido por un integrante de una organización criminal, la pena se incrementa hasta en un tercio por encima del máximo legal previsto en los supuestos anteriores. Sostengo que era innecesario, toda vez que el artículo 11.1 LDI ya lo establece en exactamente los mismos términos.

8.13. CIRCUNSTANCIAS AGRAVANTES

Son aplicables cuatro de las cinco circunstancias previstas en el artículo 11 de la Ley N.º 30096, ya que la participación específica como integrante de una organización criminal ha sido recogida explícitamente en el último párrafo del artículo 7 LDI:

i) Cometer el delito mediante el abuso de una posición especial de acceso a la data o información reservada o al conocimiento de esta información debido al ejercicio de un cargo o función. Como se ha señalado en capítulos previos, nos encontramos frente a la actuación de *insiders*.

ii) Cometer el delito con la finalidad de obtener un beneficio económico.

iii) Comprometer fines asistenciales, la defensa, la seguridad y la soberanía nacionales. En este caso, solo podría aplicarse la agravante cuando se comprometan fines asistenciales, pues la defensa, la seguridad o la soberanía nacional han sido recogidas en el tercer párrafo del propio tipo penal.

iv) Cometer el delito empleando la inteligencia artificial o tecnologías similares o análogas (conforme a la Ley N.º 32314).

8.14. PROPUESTA NORMATIVA

A partir del análisis expuesto en este capítulo, propongo modificar el delito de interceptación de datos informáticos, tomando en consideración:

i. Reformar el *nomen iuris* del delito actualmente denominado *interceptación de datos informáticos*, sustituyéndolo por *interceptación ilegal de datos informáticos y emisiones electromagnéticas*.

ii. Eliminar los elementos *deliberada* e *ilegítimamente*.

iii. Precisar que la interceptación se realiza por *medios técnicos*.

iv. Eliminar el último párrafo, por cuanto ya se encuentra previsto en el numeral 1 del artículo 11 LDI.

v. Modificar el rango de la sanción penal.

De este modo, el delito bajo estudio se regularía en los siguientes términos:

> **Art. 7.- Interceptación ilegal de datos informáticos y emisiones electromagnéticas**
>
> El que, utilizando medios técnicos, intercepta datos informáticos en transmisiones no públicas, dirigidos a un sistema informático, originados en un sistema informático o efectuado dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos, será reprimido con una pena privativa de libertad no menor de tres ni mayor de seis años.
>
> La pena privativa de libertad será no menor de cuatro ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con la Ley N.º 27806, Ley de Transparencia y Acceso a la Información Pública.
>
> La pena privativa de libertad será no menor de cinco ni mayor de diez si el delito causa o puede causar perjuicio a la defensa, seguridad o soberanía nacionales.

8.15. CONCLUSIONES DEL CAPÍTULO

- La vigilancia masiva y la pérdida de privacidad se presentan como una amenaza contemporánea. Gobiernos y empresas recolectan de forma constante datos personales como ubicación, comunicaciones, compras o relaciones sociales, con el fin de predecir y moldear el comportamiento humano. Esta recopilación, amparada por una economía basada en los datos, ha derivado en una sociedad de vigilancia, donde recuperar la privacidad se vuelve esencial para restaurar la autonomía individual y colectiva.
- El delito de interceptación ilícita de datos es reconocido internacionalmente en instrumentos como el Convenio de Budapest y la Convención de las Naciones Unidas contra la Ciberdelincuencia. A nivel nacional, esta figura penal complementa otros delitos como la interferencia telefónica y de comunicaciones electrónicas. No solo ciberdelincuentes utilizan estas técnicas: también agencias estatales lo hacen, desdibujando los límites entre la legalidad y la ilegalidad.
- Casos como el uso del *malware* AirHopper o del *spyware* Pegasus ejemplifican cómo la interceptación puede permitir la obtención de información privada en tiempo real, afectando a periodistas, activistas, políticos y ciudadanos en general. Estas prácticas han sido cuestionadas por organismos internacionales y han generado investigaciones en múltiples países, como El Salvador y Colombia.
- El artículo 3 del Convenio de Budapest establece que debe considerarse delito la interceptación técnica, deliberada e ilegítima, de transmisiones no públicas de datos informáticos, incluyendo emisiones electromagnéticas. Este delito protege la confidencialidad de la comunicación de datos y se distingue del acceso ilícito, aunque ambos comparten el mismo bien jurídico protegido.
- El Informe Explicativo del Convenio de Budapest aclara que este delito sanciona la interceptación de transmisiones electrónicas, con independencia de si los datos en sí son públicos o privados, siempre que la transmisión sea confidencial. Además, establece

que deben emplearse medios técnicos para realizar la interceptación, algo que no fue recogido por la normativa peruana, generando una diferencia conceptual relevante.

- La Convención de las Naciones Unidas contra la Ciberdelincuencia, en su artículo 8, propone una redacción similar a la del Convenio de Budapest, pero con términos ligeramente distintos, por ejemplo, *datos electrónicos* en vez de *datos informáticos*. Ambas normas coinciden en que la conducta debe ser deliberada y sin derecho.
- En el análisis comparado, algunos países como Chile, Paraguay o España siguen la línea del Convenio e incluyen la necesidad del uso de medios técnicos. Las penas varían ampliamente entre países, y los tipos penales están ubicados en capítulos distintos según el enfoque de cada legislación: intimidad, seguridad informática, patrimonio, etc.
- En Perú, tras varias propuestas legislativas, se aprobó en octubre de 2013 el artículo 7 LDI, posteriormente modificado por la Ley N.º 30171. Esta norma sanciona la interceptación ilegítima de datos informáticos con penas que oscilan entre tres y diez años, dependiendo de la gravedad del caso. La legislación distingue este delito de otros, como la interferencia de comunicaciones telefónicas o electrónicas, que se regula en los artículos 162 y 162-B del Código Penal.
- El bien jurídico protegido por esta figura penal ha sido objeto de debate. Mientras algunos sostienen que se protege la intimidad o el secreto de las comunicaciones, propongo que se trata de la confidencialidad de los datos informáticos y sistemas, alineado con la tríada de seguridad informática (confidencialidad, integridad, disponibilidad). Esto se refuerza con la distinción entre los delitos de interceptación (art. 7 LDI), interferencia (arts. 162 y 162-A CP) y acceso ilícito (art. 2 LDI).
- Una eventual reforma legislativa exige alinear el tipo penal a lo propuesto en el Convenio de Budapest y en la Convención de las Naciones Unidas contra la Ciberdelincuencia, especialmente, incluir los *medios técnicos* de comisión.

CAPÍTULO 9

ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMÁTICOS



* La ilustración de la página anterior corresponde a una adaptación de *El Infierno*, de Giovanni de Módena (1410). Para su elaboración, se empleó una de las herramientas de generación de imágenes de la empresa OpenAI.

CAPÍTULO 9

ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMÁTICOS

Sumario: 9.1. Introducción. 9.2. Regulación en el Convenio sobre la Ciberdelincuencia. 9.3. Regulación en la Convención de las Naciones Unidas contra la Ciberdelincuencia. 9.4. Legislación comparada. 9.5. Legislación nacional. 9.6. El bien jurídico penalmente protegido. 9.7. Tipicidad objetiva. 9.8. Tipicidad subjetiva. 9.9. Las situaciones de justificación en el delito de abuso de mecanismos y dispositivos informáticos. 9.10. Consumación. 9.11. Concursos. 9.12. Penalidad. 9.13. Circunstancias agravantes. 9.14. Propuesta normativa. 9.15. Conclusiones del capítulo

Usar una contraseña por lo general involucra dos componentes: presentar un desafío y recibir una respuesta. Quien desea confirmar la identidad de otra persona, pedirá la contraseña. Entonces, se supone que quien responde debe brindar un conocimiento previamente compartido y acordado entre ambas partes para demostrar su identidad. En esencia, responder correctamente el desafío de contraseña implica verificar que una persona conoce una palabra o frase específicas. Si se cree que un individuo y solo ese individuo puede saber la contraseña, entonces se asume que ese conocimiento identifica a dicha persona. Sin embargo, si la contraseña está ampliamente difundida, es probable que se produzca un error de identificación.

Las contraseñas parecieran ser incuestionables. Son omnipresentes dentro de la vida cotidiana y uno entre los varios pequeños inconvenientes de la tecnología. Aunque existen muchas organizaciones que intentan encontrar mejores modos de autenticar a los usuarios en la era globalizada de Internet, por lo general aceptamos que, a pesar de ser irritantes, las contraseñas también son necesarias, porque

> nos protegen de atacantes y nos permiten identificar a los demás a lo largo y ancho de espacios vastos.[816]

9.1. INTRODUCCIÓN

El delito de abuso de mecanismos y dispositivos informáticos está previsto en la Ley de Delitos Informáticos, dentro del capítulo denominado "Disposiciones comunes". Como veremos a continuación, la legislación nacional presenta problemas en la tipificación que pueden subsanarse siguiendo algunos ejemplos de la regulación comparada y comprendiendo el objeto de protección de este delito.

A nivel doctrinal, este ilícito se clasifica como un delito de tenencia de medios o instrumentos: "Los nuevos delitos preparatorios son básicamente, de posesión o de estatus, y muestran una fenomenología variada. Entre ellos, los más frecuentes se relacionan estructuralmente con modalidades delictivas ya clásicas. Por un lado, cabe mencionar la posesión de determinados objetos con inequívoca connotación delictiva, que enlaza la tradicional tipificación de la tenencia de útiles para el robo y de tenencia ilícita de armas. En efecto, esta estructura se ha extendido a **delitos como la posesión de programas informáticos** para la comisión de estafas o la tenencia de medios para la comisión de falsedades (art. 400 CP), entre otros ejemplos. En caso así, además, no es infrecuente que el delito preparatorio se conmine con la misma pena que el correspondiente delito de lesión consumado"[817] [El resaltado es mío]. Dicho esto, el delito bajo análisis calzaría en una manifestación de la hiperanticipación del derecho penal[818].

---

816 Eve, *Una historia de las contr43eñ4s*, cit., pp. 17.

817 Silva Sánchez, *Derecho penal. Parte general*, cit., p. 1105.

818 "Los delitos preparatorios van más allá de la tendencia a generalizar estructuras preexistentes, que tradicionalmente eran excepcionales. En efecto, en ello se tipifica además conductas que de entrada son neutras, por el mero hecho de que se lleven con una intención -una tendencia interna trascendente-delictiva (...) Al final la cuestión político-jurídica central vuelve a ser la de si se castiga una conducta o, más bien, la peligrosidad de un sujeto. Así, se habla incluso de "delitos protopreparatorios" (...) Entre las conductas típicas se cuentan (...) las de mera posesión de documentos o de acceso a contenidos de internet (...)" (Silva Sánchez, *Derecho penal. Parte general*, cit., pp. 1109 y s.).

Este delito permite sancionar tanto a quienes comercializan *malware* en galerías -a vista y paciencia de algunas autoridades- como a las organizaciones criminales que distribuyen programas maliciosos en la *dark web* y operan a nivel global, facilitando su desmantelamiento.

[Caso 116] En enero de 2025, cuando un usuario de las plataformas Cracked.io y Nulled.to ingresaban a la web, aparecía el siguiente mensaje:



Imagen 30. "Este *website* ha sido ocupado: Operación *Talent*"[819].

Cracked.io y Nulled.to fueron dos plataformas que reunieron más de 10 millones de usuarios registrados y en las que se podían adquirir credenciales de inicio de sesión robadas, herramientas para el *hacking*, servidores para alojar *malware*, entre otros programas para cometer diferentes ciberdelitos. Es más, los investigadores afirman que un producto anunciado en Cracked ofrecía acceso a miles de millones de sitios web exfiltrados. La operación tuvo lugar del 28 al 30 de enero de 2025 y se logró detener a dos personas,

819 La imagen e información ha sido tomada de: U.S. Department of Justice. *Cracked and Nulled Marketplaces Disrupted in International Cyber Operation*, publicado el 30 de enero de 2025. https://www.justice.gov/opa/pr/cracked-and-nulled-marketplaces-disrupted-international-cyber-operation

allanar siete inmuebles, incautar 17 servidores y más de 500 dispositivos electrónicos, así como 300 000 euros en efectivo y criptomonedas[820].

Para que el lector comprenda la magnitud de la operación, he de resaltar que en el operativo participó la Policía Federal australiana, la Oficina Anticibercrimen de Francia, la Oficina Federal de la Policía Criminal de Alemania, la Policía Helénica de Grecia, la Policía Estatal de Italia, la Inspección General de la Policía Rumana, la Guardia Civil y la Policía Nacional española, el Departamento de Justicia y el FBI de Estados Unidos de América.

Pese a la importancia de neutralizar la venta de dispositivos y mecanismos informáticos con fines delictivos, como en el caso que acabamos de relatar, en doctrina se cuestiona la redacción o tipificación, pues, en muchos casos, podría afectar tanto la seguridad jurídica como el principio de subsidiariedad de la intervención penal:

> Nos encontramos, en términos de Alonso de Escamilla, en un ejemplo normativo de "facilitación delictiva", que constituye un supuesto de adelantamiento en la esfera de la intervención penal [...]. Se considera así delictivos actos que no revisen suficiente desvalor de acción, atendiendo a un cuestionable elemento subjetivo de intención que desvela el interés por la comisión de los citados preceptos de descubrimiento y revelación de secretos, a modo de acto preparatorio punible, que no se contemplaba en los delitos de descubrimiento y revelación de secretos hasta la reforma del 2015. La punición de los mismos responde claramente a las indicaciones establecidas en el artículo 7 de la Directiva 2013/40/UE, del Parlamento Europeo y del consejo de la Unión Europea, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información. La Directiva se refiere así a instrumentos maliciosos, incluidos los que permiten crear redes infectadas que se utilizan para cometer ciberataques. No obstante, dicha tipificación ofrece muchas dudas desde un punto de vista político-criminal afec-

820 EUROPOL. *Law enforcement takes down two largest cybercrime forums in the world*, publicado el 30 de enero de 2025. https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-takes-down-two-largest-cybercrime-forums-in-world

> tando a la seguridad jurídica y al principio de subsidiariedad de la intervención penal, así como desde la necesidad de evitar la tipificación penal cuando estos instrumentos sean creados y comercializados con fines legítimos[821].

En este capítulo, criticaré la fórmula adoptada por el legislador peruano, pues ha extendido peligrosamente los alcances del tipo penal cuando los instrumentos internacionales recomiendan su circunscripción a determinados delitos, específicamente aquellos que atentan contra la seguridad informática.

9.2. REGULACIÓN EN EL CONVENIO SOBRE LA CIBERDELINCUENCIA

El Convenio de Budapest regula el delito de abuso de los dispositivos en el artículo 6, cuyo tenor es el siguiente:

> **Art. 6.- Abuso de los dispositivos**
>
> 1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:
>
> a. la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de:
>
> i. cualquier dispositivo, incluido un programa informático, concebido o adaptado principalmente para la comisión de cualquiera de los delitos previstos en los arts. 2 a 5 del presente Convenio;
>
> ii. una contraseña, código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático, con intención de que sean utilizados para cometer cualquiera de los delitos contemplados en los arts. 2 a 5; y
>
> b. la posesión de alguno de los elementos contemplados en los incisos i) o ii) del apartado a) del presente art. con intención de que sean utilizados para cometer cualquiera de los delitos previstos en los arts. 2 a 5.

821 Sanz Delgado, "Delincuencia cibernética y descubrimiento y revelación de secretos", cit., pp. 279 y s.

Las Partes podrán exigir en su derecho interno la posesión de un número determinado de dichos elementos para que se considere que existe responsabilidad penal.

2. No se interpretará que el presente art. impone responsabilidad penal cuando la producción, venta, obtención para la utilización, importación, difusión o cualquier otra forma de puesta a disposición mencionada en el párrafo 1 del presente art. no tenga por objeto la comisión de uno de los delitos previstos de conformidad con los arts. 2 a 5 del presente Convenio, como en el caso de las pruebas autorizadas o de la protección de un sistema informático.
3. Las Partes podrán reservarse el derecho a no aplicar el párrafo 1 del presente art., siempre que dicha reserva no afecte a la venta, distribución o cualesquiera otras formas de puesta a disposición de los elementos mencionados en el inciso 1 a) ii) del presente art.

Esta propuesta normativa presenta la siguiente estructura:

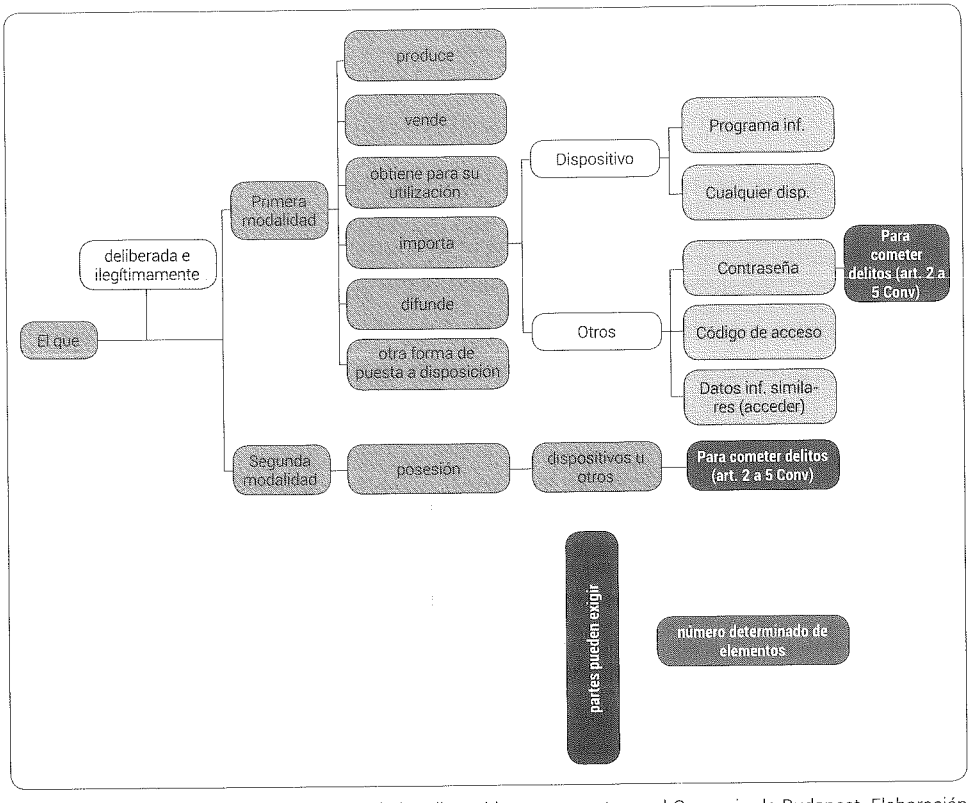


Diagrama 21. Estructura del delito de abuso de los dispositivos, propuesto en el Convenio de Budapest. Elaboración propia.

Sistemáticamente y de forma adecuada, el Convenio de Budapest ubicó el delito de abusos de dispositivos en el capítulo que protege la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos. Tiene mucho sentido, pues la intención era cubrir aquel espacio peligroso previo a la comisión de actos que atenten contra estos bienes jurídicos. Esto se ve reflejado en el parágrafo 71 del Informe Explicativo al Convenio sobre la Ciberdelincuencia[822]: "Esta disposición establece como delito separado e independiente la comisión deliberada de actos ilícitos específicos con respecto a ciertos dispositivos o datos de acceso que se utilizan mal con el fin de cometer los delitos antes descritos contra la confidencialidad, la integridad y la disponibilidad de los datos y los sistemas informáticos".

El Informe Explicativo desarrolla los alcances de este delito en los párrafos 71 al 78:

- En el párrafo 71 se señala que el objetivo de esta norma es luchar contra el mercado negro que existe alrededor de la producción y distribución de dispositivos y herramientas diseñadas para atentar contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos. Recordemos que la legislación peruana no circunscribió este ilícito a los delitos que atentan contra la seguridad informática, sino a todo aquel ilícito previsto en la LDI, es decir, amplió el ámbito de aplicación sin mayor justificación -como se analizará en este capítulo-.
- En el párrafo 72 se establece como delitos la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de un dispositivo, previstos en el Convenio [párr. 1.a).1]. Perú se aparta de la propuesta, sin mayor rigurosidad técnica, e incluye diversas modalidades no sugeridas y omite otras que sí lo fueron. Como se verá en este capítulo, esta técnica legislativa genera problemas en la interpretación y correcta subsunción normativa.
- En el párrafo 73 se da cuenta de una discusión previa sobre el alcance del compuesto lingüístico *dispositivo informático*. Así, inicialmente, se evaluó la necesidad de limitar su interpretación a

822 Council of Europe. *Convenio sobre la ciberdelincuencia. Informe explicativo*, Budapest, 23 de noviembre de 2001. https://rm.coe.int/16802fa403

aquellos que fueron diseñados exclusiva o específicamente para cometer delitos, excluyendo aquellos que presentan un uso dual. Con mucha razón, se concluyó que esta interpretación era demasiado limitada y que podría generar problemas de índole probatorio en el proceso penal.

En la misma línea, se evaluó incluir cualquier dispositivo, incluso los producidos y distribuidos de forma legal. Se rechazó esta propuesta, ya que el Convenio "restringe su alcance a los casos en los que los dispositivos son objetivamente concebidos, o adaptados, principalmente con el fin de cometer un delito".

- En el párrafo 74 se precisan las conductas que el Convenio sugiere reprimir: producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición. De estas, la legislación peruana solo acoge textualmente tres de ellas: venta, obtención para su utilización e importación. Como se analizará más adelante, nuestro país incluye modalidades adicionales.
- El párrafo 75 se refiere a la posesión de dispositivos y el número que las partes pueden (o deberían) exigir para su configuración. Este apartado es interesante, ya que explica que el número está relacionado con la intencionalidad delictiva. Lamentablemente, la legislación peruana no recoge un número mínimo de dispositivos para la configuración de este delito.
- En el párrafo 76 se aborda el elemento subjetivo del tipo. Así, si bien se destaca que la conducta debe ser deliberada -como ya se ha dicho, dolosa-, precisa que debe existir una intención específica de utilizar el dispositivo para cometer cualquiera de los delitos dirigidos contra la confidencialidad, integridad y disponibilidad. Como se puede apreciar, se recomienda incluir un elemento subjetivo de trascendencia interna. La legislación peruana sí sigue esta recomendación, pero lo hace de una forma amplia, ya que precisa que la intención del delincuente es cometer cualquier delito previsto en la LDI.
- En el párrafo 77 se recuerda que las conductas legítimas obviamente están excluidas. Así, este delito no comprende las herramientas creadas para la verificación o protección autorizada de un sistema informático, por ejemplo, dispositivos de craqueo -diseñados para

examinar los sistemas- o aquellos que sirven para verificar las redes y, así, controlar la fiabilidad de los productos.

- Finalmente, en el párrafo 78 se precisa que los Estados tienen la posibilidad de restringir sus alcances en el derecho interno. Perú fue en sentido contrario y generó un abanico mucho más amplio en la tipificación.

Algunos autores sostienen que este delito es uno de los más controvertidos de la legislación estudiada: "Además de las controversias dogmáticas con respecto a la anticipación del castigo penal al perpetrador, la discusión principal radica en el hecho de que los especialistas en seguridad informática requieren las mismas o similares herramientas (uso doble) que los cibercriminales en orden a analizar los sistemas informáticos e indagar acerca de sus debilidades. Por lo tanto, se debe poner especial énfasis en los requisitos de *mens rea* que se relacionan tanto con el objeto del delito como con la futura comisión de un delito específico contra la confidencialidad, integridad y disponibilidad de un sistema informático o datos informáticos. Sin embargo, con el tráfico ilícito de datos de contraseñas, los estrictos requisitos subjetivos han resultado ser altamente problemáticos"[823].

Al adherirnos al Convenio de Budapest, Perú se reservó el derecho de no aplicar el artículo 6, párrafo 1, literal b del Convenio, es decir, lo relacionado a la posesión de dispositivos con fines ilícitos[824]. Considero que es adecuado para evitar cualquier tipo de arbitrariedad dada la dificultad, desde el razonamiento probatorio, de acreditar el elemento subjetivo que necesariamente debería vincularse a *la intención de ser utilizado*. En esta publicación, no recomiendo incluir esta modalidad en una futura actualización legislativa.

823 Brodowski, *Cibercrimen y protección de la seguridad informática,* cit., pp. 41 y s.

824 Texto de reserva: "De conformidad con lo dispuesto en el párrafo 3 del artículo 6 del Convenio sobre la Ciberdelincuencia, la República del Perú se reserva el derecho de no aplicar el artículo 6, párrafo 1, literal b del Convenio".

9.3. REGULACIÓN EN LA CONVENCIÓN DE LAS NACIONES UNIDAS CONTRA LA CIBERDELINCUENCIA

El artículo 11 de la Convención regula el delito de uso indebido de dispositivos en los siguientes términos:

Art. 11.- Uso indebido de dispositivos

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para tipificar como delito en su derecho interno la comisión deliberada y sin derecho de los siguientes actos:
   a) La obtención, producción, venta, adquisición para su utilización, importación, distribución o cualquier otra forma de facilitación de:
      i) Un dispositivo, incluido un programa, concebido o adaptado principalmente para la comisión de alguno de los delitos tipificados con arreglo a los artículos 7 a 10 de la presente Convención; o
      ii) Una contraseña, credenciales de acceso, firma electrónica o datos similares mediante los cuales se pueda acceder a la totalidad o a una parte de un sistema de tecnología de la información y las comunicaciones, con la intención de que el dispositivo, incluido un programa, o la contraseña, las credenciales de acceso, la firma electrónica o datos similares se utilicen para cometer alguno de los delitos tipificados con arreglo a los artículos 7 a 10 de la presente Convención; y
   b) La posesión de alguno de los elementos mencionados en el párrafo 1 a) i) o ii) del presente artículo, con intención de que sea utilizado para cometer alguno de los delitos tipificados con arreglo a los artículos 7 a 10 de la presente Convención.
2. No se interpretará que el presente artículo impone responsabilidad penal cuando la obtención, producción, venta, adquisición para la utilización, importación, distribución o cualquier otra forma de facilitación o la posesión mencionada en el párrafo 1 del presente artículo no tenga por objeto la comisión de uno de los delitos tipificados con arreglo a los artículos 7 a 10 de la presente Convención, como en el caso de la realización de pruebas

autorizadas o de la protección de un sistema de tecnología de la información y las comunicaciones.

3. Cada Estado parte podrá reservarse el derecho a no aplicar el párrafo 1 del presente artículo, siempre que dicha reserva no esté relacionada con la venta, distribución ni ninguna otra forma de facilitación de los elementos mencionados en el párrafo 1 a) ii) del presente artículo.

Si bien la redacción es afín al Convenio de Budapest, se aprecian algunos cambios:

- Recoge tres conductas similares: producción, venta, importación. Reduce una: en vez de decir *obtención para su utilización*, simplemente emplea la voz *obtención*; sin embargo, agrega *adquisición para su utilización*. Reemplaza *difusión* por *distribución* y *otra forma de puesta a disposición* por *cualquier otra forma de facilitación*.
- Reemplaza la expresión *código de acceso* por *credenciales de acceso* -expresión mucho más precisa. Además, incluye la *firma electrónica* como objeto material del delito.

En cuanto a las similitudes, de forma correcta, circunscribe la comisión de este delito a los ilícitos contra la seguridad informática -como se recomienda en este libro-. Perú, lamentablemente, utiliza una fórmula amplia que entra en conflicto con el principio de lesividad.

9.4. LEGISLACIÓN COMPARADA

A continuación, analizaremos la legislación de los países que se han adherido al Convenio de Budapest y que regula el delito de abuso de mecanismos y dispositivos informáticos.

País	Legislación	Tipo penal
Países latinoamericanos que se adhirieron al Convenio de Budapest		
Ecuador	**Código Orgánico Integral Penal**	**Sección Tercera. Delitos contra la seguridad de los activos de los sistemas de la información y comunicación** **Art. 232.- Ataque a la integridad de sistemas informáticos** [...] Con igual pena será sancionada la persona que diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos, programas o sistemas informáticos maliciosos o destinados a causar los efectos señalados en el primer inciso de este artículo.

País	Legislación	Tipo penal
Brasil	Código Penal	**Seção IV. Dos Crimes contra a inviolabilidade dos segredos** **Art. 154-A.- Invasão de dispositivo informático** [...] 1. Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
Colombia	Código Penal	Título VII-A. De delitos contra el patrimonio cultural sumergido **Art. 269 E.- Uso de *software* malicioso** El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional *software* malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.
Paraguay	Código Penal	**Capítulo VII. Hechos punibles contra el ámbito de la vida y la intimidad de la persona** **Art. 146 D- Preparación de acceso indebido e interceptación de datos** 1. El que prepare un hecho punible según el Artículo 146b o el Artículo 146c produciendo, difundiendo o haciendo accesible de otra manera a terceros: 1. las claves de acceso u otros códigos de seguridad, que permitan el acceso a las en sentido del Artículo 146 b, inciso 2°; o 2. los programas de computación destinados a la realización de tal hecho, será castigado con pena privativa de libertad de hasta un año o multa. Se aplicará, en lo pertinente, lo previsto en el Artículo 266, incisos 2° y 3°.
Argentina	Código Penal	**Capítulo VII. Daños** **Art. 183.-** En la misma pena incurrirá el que [...] vendiere, distribuyere, hiciere circular [...] cualquier programa destinado a causar daños.
Chile	Ley N.° 21459	**Título I. De los delitos informáticos y sus sanciones** **Art. 8.- Abuso de los dispositivos** El que para la perpetración de los delitos previstos en los arts. 1° a 4° de esta ley o de las conductas señaladas en el art. 7° de la Ley N.° 20.009, entregare u obtuviere para su utilización, importare, difundiera o realizare otra forma de puesta a disposición uno o más dispositivos, programas computacionales, contraseñas, códigos de seguridad o de acceso u otros datos similares, creados o adaptados principalmente para la perpetración de dichos delitos, será sancionado con la pena de presidio menor en su grado mínimo y multa de cinco a diez unidades tributarias mensuales.
Costa Rica	Código Penal	**Sección VIII. Delitos informáticos y conexos** **Artículo 232.- Instalación o propagación de programas informáticos maliciosos** Será sancionado con prisión de uno a seis años quien sin autorización, y por cualquier medio, instale programas informáticos maliciosos en un sistema o red informática o telemática, o en los contenedores electrónicos, ópticos o magnéticos. La misma pena se impondrá en los siguientes casos: a) A quien induzca a error a una persona para que instale un programa informático malicioso en un sistema o red informática o telemática, o en los contenedores electrónicos, ópticos o magnéticos, sin la debida autorización. b) A quien, sin autorización, instale programas o aplicaciones informáticas dañinas en sitios de Internet legítimos, con el fin de convertirlos en medios idóneos para propagar programas informáticos maliciosos, conocidos como sitios de Internet atacantes. c) A quien, para propagar programas informáticos maliciosos, invite a otras personas a descargar archivos o a visitar sitios de Internet que permitan la instalación de programas informáticos maliciosos. d) A quien distribuya programas informáticos diseñados para la creación de programas informáticos maliciosos.

País	Legislación	Tipo penal
		e) A quien ofrezca, contrate o brinde servicios de denegación de servicios, envío de comunicaciones masivas no solicitadas, o propagación de programas informáticos maliciosos. La pena será de tres a nueve años de prisión cuando el programa informático malicioso: i) Afecte a una entidad bancaria, financiera, cooperativa de ahorro y crédito, asociación solidarista o ente estatal. ii) Afecte el funcionamiento de servicios públicos. iii) Obtenga el control a distancia de un sistema o de una red informática para formar parte de una red de ordenadores zombi. iv) Esté diseñado para realizar acciones dirigidas a procurar un beneficio patrimonial para sí o para un tercero. v) Afecte sistemas informáticos de la salud y la afectación de estos pueda poner en peligro la salud o vida de las personas. vi) Tenga la capacidad de reproducirse sin la necesidad de intervención adicional por parte del usuario legítimo del sistema informático.
Panamá	**Código Penal**	**Sección 1a. Delitos contra el derecho de autor y conexo** **Artículo 266-B.-** Se impondrá la pena de dos a cuatro años de prisión a quien fabrique, importe, distribuya, ofrezca al público, proporcione o de otra manera trafique dispositivos, productos, o componentes, u ofrezca al público o proporcione servicio, los cuales: 1. Son promocionados, publicitados, o comercializados con el propósito de evadir una medida tecnológica efectiva; o 2. Únicamente tienen un limitado propósito o uso de importancia comercial diferente al de evadir una medida tecnológica efectiva; o 3. Son diseñados, producidos o ejecutados principalmente con el fin de permitir o facilitar la evasión de cualquier medida tecnológica efectiva. Quedan excluidos del alcance de lo dispuesto en el Artículo 266-A y este artículo las bibliotecas, archivos, instituciones educativas u organismos públicos de radiodifusión no comercial sin fines de lucro.
República Dominicana	**Ley N.º 53-07**	**Capítulo I. Crímenes y delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos** **Art. 8.-** Dispositivos Fraudulentos El hecho de producir usar, poseer, traficar o distribuir, sin autoridad o causa legítima, programas informáticos, equipos, materiales o dispositivos cuyo único uso o uso fundamental sea el de emplearse como herramienta para cometer crímenes y delitos de alta tecnología, se sancionará con la pena de uno a tres años de prisión y multa de veinte a cien veces el salario mínimo.
Otras referencias		
España	**Código Penal**	**Art. 197 *ter*.-** Será castigado con una pena de prisión de seis meses a dos años o multa de tres a dieciocho meses el que, sin estar debidamente autorizado, produzca, adquiera para su uso, importe o, de cualquier modo, facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los apartados 1 y 2 del art. 197 o el art. 197 *bis*: a) un programa informático, concebido o adaptado principalmente para cometer dichos delitos; o b) una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información.

Cuadro 34. Legislación comparada respecto al abuso de mecanismos y dispositivos informáticos. Elaboración propia.

En primer lugar, se advierte que este delito se ubica en diferentes capítulos: seguridad informática, inviolabilidad de los secretos, patrimonio, dere-

chos de autor y conexos. Dicha ubicación podría influir en la identificación y delimitación del bien jurídico protegido.

En segundo lugar, a diferencia del Perú, la legislación comparada no incluye los elementos *deliberada* e *ilegítimamente* en la redacción del tipo penal analizado. Como se ha indicado a lo largo de este libro, esto no significa que se castiguen conductas culposas, sino que el resto de los países, adecuadamente, reconocen que no es necesario incluir estas expresiones para referirse a actos dolosos y que contravienen el ordenamiento jurídico.

En tercer lugar, la legislación comparada incorpora una gama más amplia de verbos que los contemplados en el Convenio de Budapest -*producir, vender, obtener para su utilización, importar, difundir* o *poner a disposición*-. Entre estos verbos adicionales se incluyen: *diseñar, desarrollar, programar, adquirir, enviar, introducir*, ejecutar, *distribuir, traficar, extraer del territorio, hacer circular, propagar* y *contratar*.

En cuarto lugar, en la legislación comparada encontramos que la acción no recae únicamente en dispositivos informáticos, contraseñas, códigos de acceso o datos informáticos que permiten el acceso a sistemas informáticos. De este modo, se incluyen otros elementos como programas, sistemas informáticos maliciosos, *software* malicioso, programas de computación de efectos dañinos, claves de acceso, códigos de seguridad, programas destinados a causar daños, programas computacionales, programas informáticos, equipos y materiales.

9.5. LEGISLACIÓN NACIONAL

9.5.1. Antecedentes normativos

Ni el Código Penal primigenio ni los proyectos de ley recibidos a fines del siglo XX desarrollaron o propusieron la tipificación de este delito.

9.5.2. Génesis legislativa

El delito de abuso de mecanismos y dispositivos informáticos nació en octubre de 2013, con la promulgación de la LDI. Cuatro proyectos de ley fueron la fuente de su tipificación:

- **Proyecto de Ley N.º 00034/2011-CR**, presentado el 11 de agosto de 2011 por el congresista Juan Carlos Eguren Neuenschwander[825]. El Convenio de Budapest propuso sancionar el uso inadecuado de *dispositivos informáticos*. En este proyecto, se adiciona el elemento *equipos*, dejándose de lado el uso de contraseñas, códigos de acceso o programas –como se propuso en proyectos posteriores–.
- **Proyecto de Ley N.º 000307/2011-CR**, presentado el 5 de octubre de 2011 por el congresista Octavio Salazar Miranda[826]. En este caso, se parte de una actuación en ausencia de autorización -requisito innecesario, pues de tenerlo, la conducta no sería ilegítima-. El autor cometería alguna de las siguientes conductas: recibir, adquirir, poseer, transferir, comercializar, distribuir, vender, controlar o custodiar elementos potencialmente dañinos. De este modo, se proponen como objetos materiales del delito: equipos de fabricación de tarjetas, instrumentos destinados a la captura, grabado, copiado o transmisión de data o información.
- **Proyecto de Ley N.º 01257/2011-CR**, presentado el 14 de junio de 2012 por el congresista Tomás Zamudio Briceño[827]. Esta

825 **Proyecto de Ley N.º 00034/2011-CR, art. 6.-** ***Prestación de equipos y servicios con fines de intrusismo y/o sabotaje.*** El que importe, fabrique, posee, distribuya, venda o utilice equipos o dispositivos con el propósito de destinarlos a vulnerar o eliminar la seguridad de cualquier sistema de información o de una tecnología de información, o el que ofrezca o preste servicios que contribuyan a ese propósito, será reprimido con pena privativa de libertad no menor de uno ni mayor de tres años.

826 **Proyecto de Ley N.º 000307/2011-CR, art. 4.-** ***Posesión de equipos de sabotaje informático.*** El que sin estar autorizado para emitir, fabricar o distribuir tarjetas magnéticas, electrónicas o inteligentes, o instrumentos análogos, reciba, adquiera, posea, transfiera, comercialice, distribuya, venda, controle o custodie cualquier equipo de fabricación de las citadas tarjetas, o de instrumentos destinados a los mismos fines o cualquier equipo o componente que capture, grabe, copie o transmita la data o información que contengan, será sancionado con pena privativa de la libertad no menor de dos ni mayor de cuatro años.

827 **CP, Art. 162-A.-** ***Tenencia ilegal de partes y equipos de interceptación de telecomunicaciones.*** El que, ilegalmente fabrica, almacena, suministra o tiene en su poder equipo de interceptación de comunicaciones o materiales destinados para su preparación, será reprimido con pena privativa de libertad no menor de 5 ni mayor de 15 años.

propuesta es la que más acota el ámbito de actuación, ya que propone sancionar únicamente aquellas conductas que recaigan sobre equipos de interceptación de comunicaciones. Si el delito fuese cometido por miembros de las Fuerzas Armadas o policías, se propuso la inhabilitación por el mismo plazo de la pena privativa de libertad.

- **Proyecto de Ley N.º 02520/2012-CR**, presentado el 26 de julio de 2013 por el presidente de la República Ollanta Humala Tasso, propuso la tipificación del artículo 208-D CP[828]. Esta iniciativa legal se aproxima mucho a la norma aprobada. Así, se pueden apreciar las conductas que fueron aceptadas: fabricar, vender, facilitar, distribuir y obtener para su utilización. Siguiendo el modelo del Convenio de Budapest, propuso limitar los delitos relacionados a este ilícito: acceso ilícito, atentados a la integridad de datos informáticos, atentados a la integridad de sistemas informáticos, fraude informático y suplantación -estos dos últimos no se encuentran en el Convenio porque no son delitos contra la seguridad informática, sino contra el patrimonio y la fe pública-.

9.5.3. Evolución legislativa

Su modificación es el resultado de tres proyectos de ley presentados:

- **Proyectos de Ley N.º 02991/2013-CR**, presentado el 25 de noviembre de 2013 por el congresista Juan Carlos Eguren Neuenschwander[829]. Recomienda incluir los elementos *deliberada* e *ilegí-*

La inhabilitación tendrá el mismo plazo que la impuesta por pena privativa de la libertad en caso que el agente activo sea funcionario público y de por vida si es miembro de las Fuerzas Armadas o policiales.

828 **Proyecto de Ley N.º 02520/2012-CR, art. 208-D.-** ***Abuso de mecanismos y dispositivos informáticos.*** El que fabrica, vende, facilita, distribuye u obtiene para su utilización mecanismos, dispositivos, contraseñas o códigos de acceso específicamente diseñados para la comisión de los delitos previstos en los artículos 197-A, 208-A, 208-B y 438-A o el que ofrece o preste servicio que contribuya a ese propósito será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días multa.

829 **Proyectos de Ley N.º 02991/2013-CR, art. 10.** ***Abuso de mecanismos y dispositivos informáticos.***- El que deliberada e ilegítimamente fabrica, diseña, desarrolla, vende,

timamente en el tipo penal. Como ya he señalado en comentarios anteriores, esta inclusión era innecesaria.

- **Proyecto de Ley N.º 02999/2013-CR**, presentado el 27 de noviembre de 2013 por el congresista Mauricio Mulder Bedoya[830]. Se propone reemplazar el verbo *fabricar* por *producir*, así como eliminar los verbos *diseñar* y *desarrollar*. Además, siguiendo el Convenio de Budapest, recomienda añadir un párrafo en el que se señalan los supuestos de ausencia de responsabilidad. Al igual que en el caso anterior, se recomienda incluir los elementos *deliberada* e *ilegítimamente*.
- **Proyecto de Ley N.º 03105/2013-CR**, presentado el 18 de diciembre de 2013 por la congresista Carmen Omonte Durand[831].

---

facilita, distribuye, importa u obtiene para su utilización, uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la presente ley, o el que ofrece o presta servicio que contribuya a ese propósito, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa.

830 **Proyecto de Ley N.º 02999/2013-CR, art.10.** ***Abuso de mecanismos y dispositivos informáticos.-*** El que de manera deliberada e ilegítima, produce, vende, obtiene para su utilización, importa, difunde o pone a disposición, cualquier dispositivo, incluido un programa informático, contraseñas, códigos de acceso o datos informáticos específicamente diseñados para la comisión de los delitos previstos en la presente ley o el que ofrece o presta servicio que contribuya a ese propósito, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días multa.
No se interpretará que el presente artículo impone responsabilidad penal cuando la producción, venta, obtención para la utilización, importación, difusión o cualquiera otra forma de puesta a disposición mencionada en el párrafo 1 del presente artículo no tenga por objeto la comisión de uno de los delitos previstos de conformidad con los artículos de la presente ley, como en el caso de las pruebas autorizadas o de la protección de un sistema informático.

831 **Proyecto de Ley N.º 03105/2013-CR, art. 10.** ***Abuso de mecanismos y dispositivos informáticos.-*** El que fabrica, diseña, desarrolla, vende, facilita, distribuye, importa u obtiene para su utilización, uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la presente ley, o el que ofrece o presta servicio que contribuya a ese propósito, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa.

No sugiere incluir los elementos deliberada e ilegítimamente, pero sí un párrafo adicional -como el proyecto anterior-, a fin de excluir ciertas conductas del ámbito penal.

9.5.4. Regulación actual

En el siguiente cuadro comparativo, compararemos la regulación originalmente aprobada con la modificación de marzo del 2014, vigente a la fecha.

Art. 10 LDI (original) Ley N.° 30096	Art. 10 LDI (actual) Modificado por la Ley N.° 30171
Art. 10. El que fabrica, diseña, desarrolla, vende, facilita, distribuye, importa u obtiene para su utilización uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la presente ley, o el que ofrece o presta servicio que contribuya a ese propósito, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días multa.	El que deliberada e ilegítimamente fabrica, diseña, desarrolla, vende, facilita, distribuye, importa u obtiene para su utilización, uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la presente ley, o el que ofrece o presta servicio que contribuya a ese propósito, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa.

Cuadro 35. Regulación del delito de abuso de mecanismos y dispositivos informáticos, 2013-2024. Elaboración propia.

Si comparamos el Convenio de Budapest, la Convención de las Naciones Unidas contra la Ciberdelincuencia y la Ley de Delitos Informáticos, veremos algunas diferencias.

	Convenio de Budapest	Convención de las Naciones Unidas contra la Ciberdelincuencia	Ley de Delitos Informáticos
	Abuso de los dispositivos (art. 6)	Uso indebido de dispositivos (art. 11)	Abuso de mecanismos y dispositivos informáticos (art. 10)
Producción	X	X	-
Venta	X	X	X
Obtención	X [para su utilización]	X	X [para su utilización]
Adquisición para su utilización	-	X	-
Importación	X	X	X
Difusión	X	-	-

No son reprimibles la producción, venta, obtención para la utilización, importación, difusión o cualquier otra forma de puesta a disposición mencionada en el presente artículo que no tenga por objeto la comisión de uno de los delitos previstos de conformidad con los artículos de la presente ley, como en el caso de las pruebas autorizadas o de la protección de un sistema informático.

	Convenio de Budapest	Convención de las Naciones Unidas contra la Ciberdelincuencia	Ley de Delitos Informáticos
Otra forma de puesta a disposición	X	-	-
Fabrica	-	-	X
Diseña	-	-	X
Desarrolla	-	-	X
Facilita	-	X	X
Distribuye	-	X	X
Ofrecer	-	-	X
Prestar servicios	-	-	X
Instrumentos			
Cualquier dispositivo	X	X	X
Programa informático	X	X	X
- **Concebido o adaptado para la comisión de delitos contra la confidencialidad, integridad y disponibilidad**	X	X	-
Contraseña	X	X	X
Código de acceso	X	-	X
Credenciales de acceso	-	X	-
Firma electrónica	-	X	-
Datos informáticos similares que permitan acceder a todo o parte de un sistema informático	X	X	-
Cualquier dato informático	-	-	X
Mecanismos	-	-	X
Finalidad genérica			
Posesión para la comisión de delitos contra la confidencialidad, integridad y disponibilidad	X	X	-
Diseñados para la comisión de los delitos previstos en la presente ley.	-	-	X

Cuadro 36. Comparación de los verbos rectores recogidos en el artículo 6 del Convenio de Budapest, el artículo 11 de la Convención de las Naciones Unidas sobre la Ciberdelincuencia y el artículo 10 de la LDI. Elaboración propia.

Perú se inclinó por una opción distinta. Así, su ubicación es un desacierto, pues localiza este delito en un capítulo denominado «Disposiciones comunes», junto a las agravantes (art. 11 LDI) y circunstancias de exención de responsabilidad (art. 12 LDI). El proyecto de Ley N.º 0034/2011 proponía ubicarlo en un capítulo denominado «Delitos contra los sistemas de información y las tecnologías de información», bajo el nombre de *prestación de equipos*

y servicios con fines de intrusismo y/o sabotaje informático. Sin embargo, el resto de proyectos de ley lo ubicaban en capítulos diferentes: el proyecto de Ley N.º 00307/2011, en un título único; el proyecto de Ley N.º 01257/2011, en el capítulo de la "Violación del secreto de las comunicaciones"; y el proyecto de Ley N.º 02520/2011 en el título "Delitos contra los datos y sistemas informáticos". Finalmente, se optó por alojarlo en un capítulo muy genérico. En este sentido, en una eventual reforma legislativa, se recomienda ubicarlo junto a los delitos de acceso ilícito, interceptación ilícita, ataques a los datos informáticos y ataques al sistema.

La tipificación del delito de abuso de mecanismos y dispositivos informáticos en la legislación penal peruana presenta la siguiente estructura:

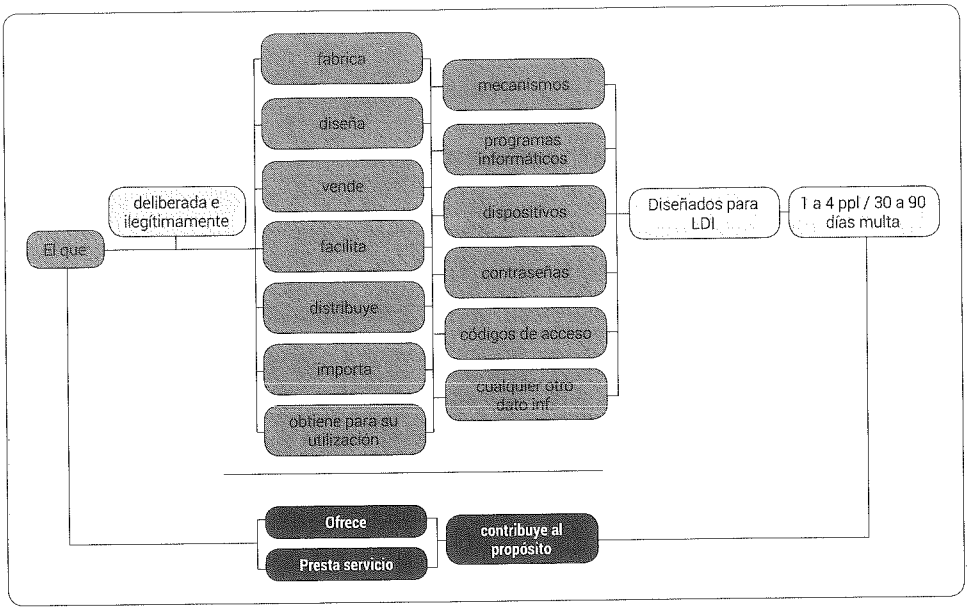


Diagrama 22. Estructura actual del delito de abuso de dispositivos y mecanismos informáticos, en el sistema penal peruano. Elaboración propia.

9.6. EL BIEN JURÍDICO PENALMENTE PROTEGIDO

Toda vez que este delito se aleja de una efectiva lesión al bien jurídico adopta la forma de un delito de peligro abstracto[832].

832 Oré Sosa, *Delictum. Apuntes de derecho penal*, cit., p. 210.

La doctrina nacional identifica el bien jurídico a proteger penalmente con el objeto de protección: "Los bienes jurídicos protegidos en este delito son diversos y dependen del tipo de dispositivo y la finalidad de su fabricación o utilización"[833]. En similar posición: "Estamos en condiciones de señalar que su bien jurídico protegido dependerá de los ciberdelitos que facilite. En esa medida, por ejemplo, si se tratara de los delitos de acceso ilícito y atentados contra datos/sistemas informáticos hablaríamos solo del bien jurídico 'integridad informática'. Empero si se tratara de interceptación de datos informáticos, el bien jurídico sería plural y hablaríamos de la integridad informática, la intimidad y el secreto de las comunicaciones"[834]. En la misma línea, debido a la errónea ubicación de este delito en la LDI, se afirma que "el bien jurídico protegido por esta norma penal no tiene la característica de ser unitario ni específico, sino que va a estar condicionado al caso concreto, esto es, según el delito informático que se haya cometido"[835].

La decisión del legislador no es adecuada. Anticipar la barrera punitiva, en los términos recogidos en la LDI, genera inseguridad jurídica y puede ocasionar abusos. Esto se origina porque no se comprende el sentido de la criminalización de esta conducta específica, pero, sobre todo, no se determina cuál es el bien jurídico que en este caso se debe proteger.

¿Existen programas creados específicamente para cometer suplantaciones de identidad (art. 9 LDI), *grooming* (art. 5 LDI), chantaje sexual con materiales elaborados o modificados por medios digitales (art. 5-A LDI) o préstamos informáticos extorsivos (art. 8-A LDI)? En realidad, en todos estos casos se utilizan programas, herramientas, mecanismos o dispositivos legales para cometer actos ilegales, pues son ciberdelitos réplica.

Dicho esto, la razón de este tipo penal no es anticiparse al mal uso de las TIC para facilitar la comisión de delitos tradicionales, sino un grupo en particular: la ciberdelincuencia pura. De este modo, el bien jurídico a proteger será la seguridad informática.

833 Espinoza Calderón, *Delitos informáticos y nuevas modalidades delictivas*, cit., p. 102.

834 Arévalo Minchola/Vega Aguilar, *Ciberdelitos. Análisis en el sistema penal*, cit., p. 374.

835 Jiménez Herrera, *Manual de derecho penal informático*, cit., p. 476.

Delitos contra la seguridad informática		
Hiperanticipación	**Confidencialidad**	**Integridad/Disponibilidad**
Abuso de mecanismos y dispositivos informáticos (art. 10 LDI)	Acceso ilícito (art. 2 LDI)	Daños informáticos (art. 3 LDI)
	Interceptación ilícita de datos (art. 7 LDI)	Sabotaje informático (art. 4 LDI)

Cuadro 37. Sistematización de los ciberdelitos contra la seguridad informático, según el bien jurídico afectado específicamente. Elaboración propia.

Adelantar la barrera punitiva genera tensiones con el principio de lesividad, por eso su tipificación debe ser cuidadosamente estudiada y su ubicación, adecuada. De ahí que tanto el Convenio de Budapest[836] como la Convención de las Naciones Unidas[837] y otros instrumentos internacionales[838] restrinjan sus alcances a los delitos que atentan específicamente contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos.

836 El **art. 6** del Convenio expresamente dice: "Con intención que sean utilizados para cometer cualquiera de los delitos contemplados en los artículos 2 a 5". Recordemos que estos son: acceso ilícito (**art. 2**), interceptación ilícita (**art. 3**), ataque a la integridad de los datos (**art. 4**) y ataque a la integridad del sistema (**art. 5**).

837 El **art. 7** de la Convención prevé: "[...] se utilicen para cometer alguno de los delitos tipificados con arreglo a los artículos 7 a 10 de la presente Convención". Los delitos son: Acceso ilícito (**art. 7**), interceptación ilícita (**art. 8**), interferencia con datos electrónicos (**art. 9**) e interferencia con un sistema de tecnología de la información y las comunicaciones (**art. 10**).

838 "Los delincuentes cibernéticos también pueden producir poseer y/o distribuir herramientas informáticas de uso indebido, incluidos dispositivos tecnológicos, *software* malicioso (o *malware*) y contraseñas, códigos de acceso y otros datos que permitan a las personas obtener acceso ilegal, interceptar o interferir de otra manera con el objetivo. El artículo 9 (delito de uso indebido de medios de tecnología de la información) de la Convención Árabe para el Combate de los Delitos relacionados con las Tecnologías de la Información penaliza: "(1) La producción, venta, compra, importación, distribución o provisión de. (a) cualquier herramienta o programa diseñado o adaptado con el fin de cometer los delitos señalados en los artículos 6 [(delito de acceso ilícito), artículo 7 (delito de interceptación ilícita) y artículo 8 (delito contra la integridad de los datos)] [...] (b) la contraseña de sistemas de información, código de acceso o información similar que permita el acceso al sistema de información con el fin de utilizarlo para cualquiera de los delitos señalados en los artículos 6 a 8 [...] [y] (2) la adquisición de cualquiera de las herramientas o programas mencionados en los dos párrafos anteriores, con el fin de utilizarlos para cometer cualquiera de los delitos señalados en los artículos 6 a 8"." (UNODC. *Ciberdelito I: Guía práctica para un abordaje integral del fenómeno. Tipos generales. Marco jurídico y derechos humanos. El ABC de la investigación*. Lima: 2022, p. 43).

9.7. TIPICIDAD OBJETIVA

9.7.1. Sujetos

Estamos frente a un delito común, por lo que el sujeto activo puede ser cualquier persona, no exigiéndose una condición técnica específica.

Pese a ello, la doctrina nacional ha sostenido que "sujeto activo de este delito pueden ser personas con alto nivel intelectual en el manejo de la informática, inclusive con estudios superiores en la materia, cuyo conocimiento es usado para facilitar la comisión de delitos informáticos"[839].

En estos casos, la doctrina adecuadamente ha reconocido que aquellas personas que no tienen conocimientos especializados en informática compran o adquieren herramientas o programas que les permitirá cometer delitos informáticos: "Se castiga, por tanto, a quien fabrica un *malware* malicioso con la intención de que sea utilizado para causar un daño informático grave, de los considerados delictivos, a quien adquiere con tal fin, a quien lo facilita a un tercero, a quien descubriendo una vulnerabilidad diseña un programa de ataque DoS, con la intención de cometer o favorecer la comisión de un delito del art. 264 bs, etc."[840].

9.7.2. Acción típica

El artículo 10 LDI recoge dos modalidades claramente diferenciadas:

a) Abuso de dispositivos informáticos, que incluyen fabricar, diseñar, vender, facilitar, distribuir, importar y obtener para su utilización.

b) Ofrecimiento y prestación de servicios ilícitos. Esta modalidad atenta contra el principio de lesividad por tratarse de la que más se aleja de cualquier daño que podría cometerse al anticiparse excesivamente la barrera de punibilidad. Además, con mucha razón se critica la decisión del legislador de equiparar un acto de colaboración con la autoría misma:

839 Espinoza Calderón, *Delitos informáticos y nuevas modalidades delictivas*, cit., p. 104.

840 Gil Gil, "Daños informáticos", cit., p. 505.

> Propio de estos tiempos es la sanción, como autor, de conductas que materialmente son de complicidad o cooperación en el delito. Y aunque desde una perspectiva normativa también ha de imputarse al partícipe la infracción de una norma, la entidad de la misma no parece ostentar una relevancia suficiente como para sancionar, por ejemplo, el simple ofrecimiento de contribuir a la comisión de los delitos. Por lo demás, ni siquiera debería ser considerado como un acto de intervención por manifestarse de modo previo a la propia fase de preparación del delito[841].

Una eventual reforma legislativa debería eliminar esta última modalidad y circunscribirse a los verbos rectores recomendados en el Convenio de Budapest y en la Convención de las Naciones Unidas contra la Ciberdelincuencia.

Luego de efectuar esta breve crítica, analizaremos cada verbo rector de la primera modalidad y se propondrán definiciones que eviten contradicciones y que cubran, de alguna forma, todo el abanico posible de conductas reprochables.

9.7.2.1. Fabricar

Este verbo no es propuesto ni por el Convenio de Budapest ni por la Convención de las Naciones Unidas contra la Ciberdelincuencia. No obstante, ambos instrumentos recogen un verbo similar: *producir*.

A nivel local, se entiende que *fabricar* implica construir o elaborar dispositivos[842] como decodificadores de señales digitales o programas de cómputo para interceptar comunicaciones[843]. Según un sector de la doctrina, entre estas acciones se encontrarían las siguientes: confeccionar, elaborar, transformar, crear forjar, producir o inventar de manera deliberada e ilegítima elementos como *software* de *hacking*, contraseñas, programas informáticos o similares[844]. En cambio, otra postura doctrinal restringe esta noción al plano físico, ya que

841 Oré Sosa, *Delictum. Apuntes de derecho penal*, cit., p. 211.

842 Espinoza Calderón, *Delitos informáticos y nuevas modalidades delictivas*, cit., p. 103.

843 Arévalo Minchola/Vega Aguilar, *Ciberdelitos. Análisis en el sistema penal*, cit., p. 374.

844 Jiménez Herrera, *Manual de derecho penal informático*, cit., p. 479.

la relaciona con la construcción y elaboración de *hardware* para la comisión de delitos informáticos, descartando así el aspecto virtual[845].

En este contexto, el verbo *fabricar* podría entrar en tensión con otros como *desarrollar*, que suele asociarse con el *software*. Para superar cualquier contradicción o superposición, por *fabricar* entenderemos la construcción de un objeto físico malicioso, a partir de determinados insumos o componentes, que puede ser empleado en un ciberataque.

A continuación, describiré una historia imaginaria para comprender el proceso de fabricación.

[Caso 117] Cansado de su rutinario trabajo como asistente técnico en un centro universitario, Julián -un joven ingeniero trujillano de 27 años- empezó a fantasear con crear algo que rompiera la monotonía. Una noche, mientras exploraba foros de ciberseguridad en la red, se topó con los planos de un USB Killer. Intrigado por su simplicidad destructiva, decidió construir uno por su cuenta. En una tienda de electrónica local compró condensadores cerámicos, un transistor MOSFET, resistencias y una pequeña placa PCB. Por internet encargó un microcontrolador ATtiny85 y carcasas de pendrive genéricas para camuflar su creación.

Durante varias semanas, ensambló minuciosamente el dispositivo en su pequeño taller casero: soldó los componentes, programó el microcontrolador para que cargara rápidamente los condensadores al conectarse a un puerto USB y descargara la energía en un pulso letal sobre la placa madre del equipo objetivo. Una mañana, aprovechando que nadie lo observaba, conectó su primer prototipo al puerto de una computadora de uso común en la sala de profesores. En pocos segundos, la pantalla parpadeó y luego murió, junto con todo el equipo. Julián sonrió, no por malicia, sino por la extraña satisfacción de haber creado algo funcional con sus propias manos.

845 Meneses Gonzáles/Meneses Ochoa, *La cibercriminalidad: consideración criminológica, político-criminal, dogmática, procesal y cooperación internacional*, cit., p. 337.

9.7.2.2. Diseñar

Este verbo no es propuesto ni por el Convenio de Budapest ni por la Convención de las Naciones Unidas contra la Ciberdelincuencia.

Se entiende que quien diseña "planifica de acuerdo a la necesidad de su uso"[846] e "implica hacer un plan detallado, una estructura de los principales dispositivos a utilizarse en la interceptación de comunicaciones"[847]. De este modo, estaríamos frente a "una actividad creativa, realizada por el individuo que tiene por fin proyectar objetos, logotipos, programas, *software*, para que después sean fabricados"[848]. Así, en general, se afirma que "esta acción está relacionada con la creación de elementos de *hardware* o *software* destinados a la comisión de ilícitos informáticos" [849].

Como se puede apreciar, esta actividad tiene un carácter netamente preparatorio, previo tanto a la fabricación del *hardware* como al desarrollo efectivo del *software* malicioso. Desde esta perspectiva, sancionar penalmente el diseño -entendido como fase preliminar, desvinculada aún de la ejecución concreta- podría vulnerar el principio de lesividad, pues se estaría anticipando la punibilidad a una etapa en la que el bien jurídico tutelado (seguridad informática) no ha sido todavía puesto en riesgo real.

Por lo tanto, incluir el diseño como conducta típica sin una clara conexión con un peligro concreto podría implicar una expansión injustificada del derecho penal.

[Caso 118] Marc Goodman describe el caso de una empresa que, aunque aparenta ser una compañía de servicios, en realidad desarrolla *software* y *hardware* ilegales, operando dentro del mercado negro: "Del mismo modo que las empresas legales contratan a programadores informáticos para armar sus sitios web y programar *software*, también lo hace Crime S. A. Una empresa como CrimeEnforcers (un juego de palabras con *law enforcers*,

846 Espinoza Calderón, *Delitos informáticos y nuevas modalidades delictivas*, cit., p. 103.

847 Arévalo Minchola/Vega Aguilar, *Ciberdelitos. Análisis en el sistema penal*, cit., p. 374.

848 Jiménez Herrera, *Manual de derecho penal informático*, cit., p. 479.

849 Meneses Gonzáles/Meneses Ochoa, *La cibercriminalidad: Consideración criminológica, político-criminal, dogmática, procesal y cooperación internacional*, cit., p. 337.

'cuerpos de seguridad') se describe como una 'organización privada para tus solicitudes de desarrollo especiales [...]. Si necesitas *hardware* especial [...] o *software* que no pueda realizarse o incluso debatirse [sic] en tu país [...], te ofrecemos programación completamente anónima y en el extranjero para tus proyectos. Nos da igual qué pretendas hacer con el *hardware* y el *software* que nos solicites. Es decir, que en el mundo del desarrollo de *software* con fines delictivos no se formulan preguntas'"[850].

He propuesto este caso como un ejemplo de diseño de dispositivos y mecanismos ilegales, basado en el hecho de que la empresa ofrece tomar la idea del cliente y desarrollar una solución. Si la misma persona lleva a cabo su implementación, estaríamos ante un caso de producción, ya que el diseño es la etapa previa a esta.

9.7.2.3. Desarrollar

Este verbo no es propuesto ni por el Convenio de Budapest ni por la Convención de las Naciones Unidas contra la Ciberdelincuencia. No obstante, como ya se ha indicado, ambos instrumentos recogen un verbo similar: *producir*.

En la doctrina local encontramos por lo menos dos propuestas de definición. De un lado, se define *desarrollar* como hacer "más sofisticado y difícil de detectar"[851], esto es, "mejorar o reforzar algo que se ha venido planeando. De este modo, se sostiene que el agente ya tiene el mecanismo, dispositivo o programa y lo que hace es aumentar su eficacia para que se use en actividades criminales"[852]. Otro sector considera que "esta acción la asociamos a la participación en el proceso desde la creación de *software* y/o *hardware* dirigido a la comisión de delitos informáticos" [853]. Como se puede advertir, nos encontramos frente a un problema: ¿por desarrollar debemos entender una mejora o la generación de un producto nuevo?

850 Goodman, *Los delitos del futuro. Todo está conectado. Todos somos vulnerables. ¿Qué podemos hacer al respecto?*, cit., pp. 329 y s.

851 Espinoza Calderón, *Delitos informáticos y nuevas modalidades delictivas*, cit., p. 103.

852 Arévalo Minchola/Vega Aguilar, *Ciberdelitos. Análisis en el sistema penal*, cit., p. 374.

853 Meneses Gonzáles/Meneses Ochoa, *La cibercriminalidad: Consideración criminológica, político-criminal, dogmática, procesal y cooperación internacional*, cit., p. 337.

Considero que estas propuestas no son adecuadas:

a) Sancionar el incremento o mejora de las funcionalidades de una herramienta ilegal es innecesario, ya que recibiría exactamente la misma pena quien construye un mecanismo como quien lo mejora. Esto no significa que el acto quede impune, pues podrá ser sancionado bajo las conductas que ya hemos definido: diseño o fabricación.

b) La segunda definición presenta problemas, ya que se superpone con los alcances de fabricar -que, en esta obra, lo describimos como el proceso de construcción del aspecto físico del dispositivo-.

De este modo, para evitar contradicciones, propongo interpretar el verbo *desarrollar* como la creación de *software ilegal* que no requiere un soporte físico. Así, *fabricar* hará referencia al aspecto físico, mientras que *desarrollar* al ámbito virtual.

[Caso 119] Imaginemos que dos empresas ofrecen el mismo producto a un usuario, quien debe elegir entre uno y solo uno. Por ejemplo, si buscas un televisor para tu sala, tendrás que decidir entre los distintos modelos disponibles en la tienda que visites.

Algo similar ocurre en el mercado negro, pero con *malware*. Dos programas maliciosos pueden competir por infectar y controlar el mismo dispositivo. Sin embargo, la víctima, sin saberlo, tiene su computadora comprometida. ¿Cómo se resuelve esta competencia? Uno de los desarrolladores decidió *mejorar* su *malware* para que pudiera detectar y eliminar a su rival, asegurándose así el control exclusivo del sistema infectado. Este fue precisamente el caso de SpyEye y Zeus, dos troyanos bancarios que libraron una batalla en el mundo del cibercrimen para monopolizar la infección de dispositivos.

SpyEye y Zeus competían por dominar el mercado negro del *malware*. Los desarrolladores de SpyEye identificaron una oportunidad para obtener ventaja: mejorar su *software* malicioso incorporando un mecanismo similar a un antivirus. Esta nueva función permitía detectar la presencia de Zeus en un dispositivo infectado, eliminarlo y reparar el punto de acceso utilizado, impidiendo que volviera a infiltrarse. De este modo, SpyEye aseguraba el

control exclusivo del sistema, consolidándose como el único troyano bancario operando en la máquina comprometida[854].

[Caso 120] A continuación, analizaremos un caso de negocio ilegal en el que la idea de una empresa, inicialmente concebida para ofrecer un servicio, terminó evolucionando hasta convertirse en un producto ilícito, específicamente en un *malware*.

CallService.biz es un servicio diseñado para ciberdelincuentes, ofreciendo intérpretes en inglés, francés y alemán bajo demanda. Su principal función es ayudar a los delincuentes a obtener información sensible, como claves de acceso y medidas de seguridad de los usuarios, permitiéndoles así acceder a cuentas bancarias, correos electrónicos o redes sociales. Este servicio opera de manera similar a un *call center*, funcionando las 24 horas del día, los siete días de la semana. De este modo, se convierte en un centro de asistencia plurilingüe delictivo, disponible para cualquier criminal que desee contratar sus servicios[855].

Compañías similares han recopilado, estructurado en paquetes y desarrollado programas maliciosos con el mismo propósito. En este contexto, nos encontramos ante el *desarrollo* de *malware* como parte del modelo Crime as a Service (CaaS), donde la ciberdelincuencia se ofrece como un servicio accesible para terceros.

9.7.2.4. Vender

Este verbo sí es propuesto tanto por el Convenio de Budapest como por la Convención de las Naciones Unidas contra la Ciberdelincuencia.

854 Goodman, *Los delitos del futuro. Todo está conectado. Todos somos vulnerables. ¿Qué podemos hacer al respecto?*, cit., p. 332.

855 Goodman, *Los delitos del futuro. Todo está conectado. Todos somos vulnerables. ¿Qué podemos hacer al respecto?*, cit., p. 330.

Vender hace referencia a lucrar con su venta[856], "dar una cosa a alguien a cambio de una determinada cantidad de dinero"[857] o "traspasar, despachar, subastar, liquidar, u otro análogo, cualquier mecanismo o dispositivo informático, como alguna contraseña para romper las medidas de seguridad de una base de datos o sistema informático, pero que ese acto sea con la condición de recibir un beneficio económico (dinero), es decir, que es necesario que se actúe bajo un ánimo de lucro"[858]. En este sentido, se sanciona al "que comercializa datos informáticos, así como *software* o *hardware* destinado a la comisión de delitos informáticos" [859].

[Caso 121] Al comienzo de este capítulo mencioné dos plataformas donde los usuarios podían adquirir *malware* y otros programas maliciosos. A continuación, exploraremos tres de estos programas que, hace una década, alcanzaron gran popularidad entre los compradores[860]:

- **Zeus Builder.** Este programa se vendía entre cinco mil y siete mil dólares dada sus funciones: desde capturar pulsaciones del teclado (*keylogger*) hasta obtener los certificados de encriptación digitales requeridos por la banca en línea. Según los cálculos, este troyano habría infectado cerca de trece millones de ordenadores a nivel mundial.
- **Bugat.** Los usuarios podían adquirir este *malware* por mil dólares, cuya función era usurpar cuentas bancarias y simular solicitudes de transferencias. En el 2010, fue empleado en una campaña masiva de *phishing*: los atacantes enviaron correos a decenas de millones de usuarios de LinkedIn bajo el mensaje «Actualiza tu cuenta». En menos de cuatro segundos, Bugat se instalaba y permanecía latente a la espera de los datos financieros.

856 Espinoza Calderón, *Delitos informáticos y nuevas modalidades delictivas*, cit., p. 103.

857 Arévalo Minchola/Vega Aguilar, *Ciberdelitos. Análisis en el sistema penal*, cit., p. 375.

858 Jiménez Herrera, *Manual de derecho penal informático*, cit., p. 481.

859 Meneses Gonzáles/Meneses Ochoa, *La cibercriminalidad: Consideración criminológica, político-criminal, dogmática, procesal y cooperación internacional*, cit., p. 337.

860 Goodman, *Los delitos del futuro. Todo está conectado. Todos somos vulnerables. ¿Qué podemos hacer al respecto?*, cit., p. 330.

- **SpyEye.** Este *malware* contaba con las funciones de Zeus Builder, pero costaba tan solo 500 dólares. Como vimos, líneas arriba, para imponerse sobre la competencia, los desarrolladores del SpyEye lo actualizaron con un antivirus para que eliminase Zeus de los dispositivos infectados y ser el único que lo controlaba.

9.7.2.5. Facilitar

La Convención de las Naciones Unidas contra la Ciberdelincuencia recoge una fórmula similar: *cualquier otra forma de facilitación*. Si bien el Convenio de Budapest no emplea la voz *facilitar*, sí utiliza una expresión afín: *puesta a disposición*. En esta línea, el parágrafo 72 del Informe Explicativo del Convenio de Budapest, desarrolla la referida expresión en los siguientes términos:

> La puesta a disposición se refiere al poner en línea dispositivos para ser utilizados por otras personas. Este término propone también abarcar la creación o compilación de hipervínculos con el fin de facilitar el acceso a dichos dispositivos.

La doctrina local entiende que *facilitar* es "hacer fácil o posible la ejecución de algo o la consecución de un fin. Esta facilitación que se realiza siempre versará sobre el ciberdelito a cometer"[861]. Se sostiene que quien facilita no participa de forma directa, en tanto su actividad consiste en "proporcionar o entregar o de hacer fácil o posible la ejecución"[862]. Creo que estas definiciones resultan útiles para un primer acercamiento, pero son insuficientes para capturar la especificidad técnica y jurídica que demanda el entorno digital.

Si acudimos a la Real Academia de la Lengua, veremos que facilitar tiene dos acepciones: (i) hace fácil o posible la ejecución de algo o la consecución de un fin; y (ii) proporcionar o entregar. La primera acepción recoge los siguientes sinónimos: *simplificar*, *posibilitar*, *permitir*, *favorecer*, *ayudar*, *allanar*; en tanto, la segunda acepción: *entregar*, *suministrar*, *proveer* o *surtir*. Esta interpretación

861 Arévalo Minchola/Vega Aguilar, *Ciberdelitos. Análisis en el sistema penal*, cit., p. 375.

862 Jiménez Herrera, *Manual de derecho penal informático*, cit., p. 482.

literal tampoco ayuda mucho, pues los actos de colaboración se sancionan bajo la figura de complicidad primaria o secundaria.

Este escenario cambia, si leemos el Convenio de Budapest en inglés, uno de los idiomas oficiales: "The production, sale, procurement for use, import, distribution or otherwise making available of [...]". De estos verbos, considero que el último nos permitirá conferirle un significado propio. Así, por *facilitar* entenderemos *making available*. Es decir, poner a disposición de terceros herramientas tecnológicas diseñadas para la comisión de delitos informáticos, sin que ello implique necesariamente su entrega directa, venta o distribución individualizada. Por ejemplo, si en un foro un ciberdelincuente publica una entrada explicando que ha desarrollado un determinado *malware* y sube el archivo para que cualquiera pueda descargarlo y utilizarlo con fines ilícitos, podrá afirmarse que lo ha facilitado. Esta conducta, aunque distinta de la venta o distribución directa, constituye una forma de colaboración técnica previa y deliberada. La definición propuesta evita conflictos interpretativos.

[Caso 122] El 22 de enero de 2025, el usuario @Alph4_Sec publicó en la red social X el siguiente mensaje: "El grupo Deface Peru ha publicado credenciales de acceso al Sistema Único de Gestión Administrativa (SUGA) de la Corte Superior de Justicia de Arequipa, exponiendo la seguridad del sistema". Además, colocó la siguiente imagen:

Si se comprobara que, a través de un blog, página web o red social, se están difundiendo los usuarios y contraseñas de una corte de justicia de nuestro país, el responsable habría incurrido en el delito de distribución de mecanismos y dispositivos informáticos, específicamente en la modalidad de *facilitar* contraseñas.

De otro lado, si una persona ajena a la Corte Superior de Justicia de Arequipa toma nota del usuario y de la contraseña y accede al sistema de dicha corte, comete el delito de intrusismo informático, en la modalidad de acceso con vulneración de las medidas de seguridad.

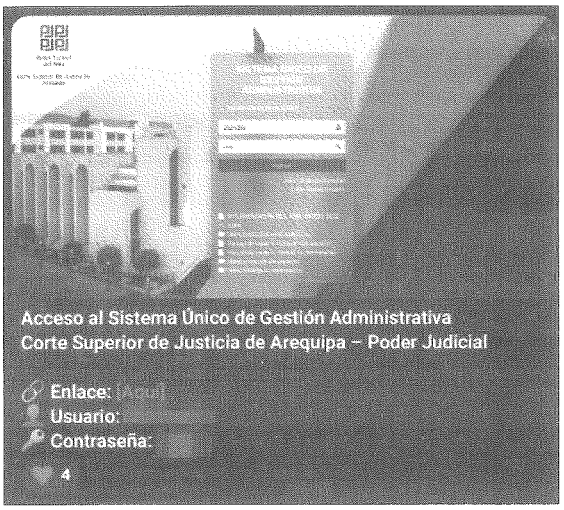


Imagen 31. Publicación obtenida en la red social X que reflejaría un posible ataque cibernético a la Corte Superior de Justicia de Arequipa[863].

9.7.2.6. Distribuir

Aunque en la versión en español del Convenio de Budapest se utiliza la palabra *difusión*, en su versión oficial en inglés se emplea el verbo *to distribute* (*distribution*). Esta diferencia no es menor, ya que el término *distribuir* también es recogido por la Convención de las Naciones Unidas contra la Ciberdelincuencia. De hecho, el parágrafo 72 del Informe Explicativo del Convenio de Budapest aclara que *distribuir* se refiere al acto de enviar datos a terceros, lo cual aporta una mayor precisión respecto al alcance de esta conducta.

En el ámbito local, se entiende que, al distribuir, el agente empieza a hacer circular los dispositivos y entregar estos mecanismos a otras personas para que lo puedan comercializar y/o ubicar[864]. Así, se sostiene que quien distribuye "va a repartir o entregar mecanismos y/o dispositivos informáticos, como programas informáticos o *software* realizados específicamente para la comisión de un delito

863 La publicación data del 22 de enero del 2025 y puede ser visualizada a través del siguiente enlace: https://x.com/alph4_sec/status/1882212136426037293?s=61

864 Arévalo Minchola/Vega Aguilar, *Ciberdelitos. Análisis en el sistema penal*, cit., p. 375.

informático"[865]. En esta línea, otros autores definen *distribuir* como "la acción de entregar *software* o *hardware* para ilícitos informáticos" [866].

Para superar las eventuales contradicciones terminológicas, en este trabajo se propone entender *distribuir* como todo acto de entrega de *hardware o software* malicioso a terceros, sin que necesariamente implique una transacción económica. Esta interpretación permite abarcar modalidades como el obsequio, el préstamo o la transferencia de posesión, y se alinea tanto con el sentido funcional del verbo en el Convenio de Budapest como con la práctica observada en contextos locales.

9.7.2.7. Importar

Este verbo sí es propuesto tanto por el Convenio de Budapest como por la Convención de las Naciones Unidas contra la Ciberdelincuencia.

La voz *importar* se refiere a comprar en otro país[867]. De este modo, la doctrina nacional lo define como la acción de "comprar en el extranjero y traerlo al país para su consumo. En el caso específico se referirá a la acción de adquirir dispositivos o mecanismos en un país extranjero y utilizarlo en nuestro país para la comisión de ciberdelitos"[868]. Se sostiene que la importación podría ser física o por el ciberespacio, "aunque mayormente se da en el primer caso, de que ingresan al país programas informáticos, *software* o discos que contienen contraseñas o códigos de acceso"[869].

Este verbo no genera mayor controversia. En tal sentido, coincido con la definición propuesta por Meneses Gonzáles y Meneses Ochoa: "Comprar del extranjero *software* o *hardware* para la comisión de delitos informáticos" [870].

---

865 Jiménez Herrera, *Manual de derecho penal informático*, cit., p. 483.

866 Meneses Gonzáles/Meneses Ochoa, *La cibercriminalidad: Consideración criminológica, político-criminal, dogmática, procesal y cooperación internacional*, cit., p. 337.

867 Espinoza Calderón, *Delitos informáticos y nuevas modalidades delictivas*, cit., p. 103.

868 Arévalo Minchola/Vega Aguilar, *Ciberdelitos. Análisis en el sistema penal*, cit., p. 375.

869 Jiménez Herrera, *Manual de derecho penal informático*, cit., pp. 484 y s.

870 Meneses Gonzáles/Meneses Ochoa, *La cibercriminalidad: Consideración criminológica, político-criminal, dogmática, procesal y cooperación internacional*, cit., p. 337.

[Caso 123] En una pequeña habitación de Lima, rodeados de laptops, pantallas divididas y ventiladores que apenas mitigaban el calor, cuatro jóvenes peruanos -todos con formación técnica autodidacta- diseñaban su próximo gran golpe. Tras meses estudiando las herramientas de ciberespionaje más modernas. Se obsesionaron con el USB-C O.MG, un cable aparentemente inofensivo, pero con un poder devastador: permitir acceso remoto al dispositivo del usuario. Recurriendo a foros ocultos y canales de mensajería cifrada, contactaron a un proveedor extranjero que les ofrecía un ciento de unidades desde China y otra tanda más costosa desde Estados Unidos. Utilizando empresas fantasmas para no levantar sospechas, lograron importar discretamente los cables ocultos en cargadores de teléfonos, con destino final a los mercados informales de tecnología en Lima y provincias.

Una vez en sus manos, el grupo desplegó una campaña de venta camuflada. A través de cuentas falsas en Facebook Marketplace, grupos de Telegram y canales de venta por WhatsApp, ofrecieron cargadores y cables USB-C de alta velocidad y con chip de carga rápida a precios imposibles de ignorar. También lograron infiltrar algunos lotes en *stands* físicos en mercados populares como Wilson y Las Malvinas, donde los vendedores, sin saber que estos eran dispositivos maliciosos, los revendían. Algunos compradores incluso los adquirieron convencidos de que eran cables originales de marcas *premium*, debido al empaque cuidadosamente replicado. Para los ciberdelincuentes, el éxito no era solo económico: una vez conectados, los cables les permitían activar comandos, registrar teclas o incluso abrir sesiones remotas en los dispositivos infectados.

Luis Alberto, un diseñador gráfico *freelance* de Arequipa, fue una de las víctimas. Había comprado el cable en línea por menos de la mitad de lo que costaba uno original. Todo parecía normal hasta que notó que su laptop enviaba correos extraños y sus cuentas empezaron a bloquearse por *intentos sospechosos*. Pese a reinstalar el sistema operativo, los accesos no cesaban. La clave estaba en el cable mismo: desde el primer día, había abierto una puerta silenciosa a su sistema. Su información bancaria, redes sociales y proyectos laborales habían sido vulnerados. La frustración lo llevó a denunciar el caso, aunque era casi imposible rastrear el origen del ataque.

El USB-C O.MG es un dispositivo que se ve y actúa como un cable común, pero contiene en su interior un microcontrolador capaz de registrar pulsaciones del teclado, ejecutar comandos maliciosos o incluso abrir túneles de acceso remoto. A simple vista es indistinguible de un cable común, lo que lo convierte en una de las herramientas más sofisticadas del *hacking* físico.

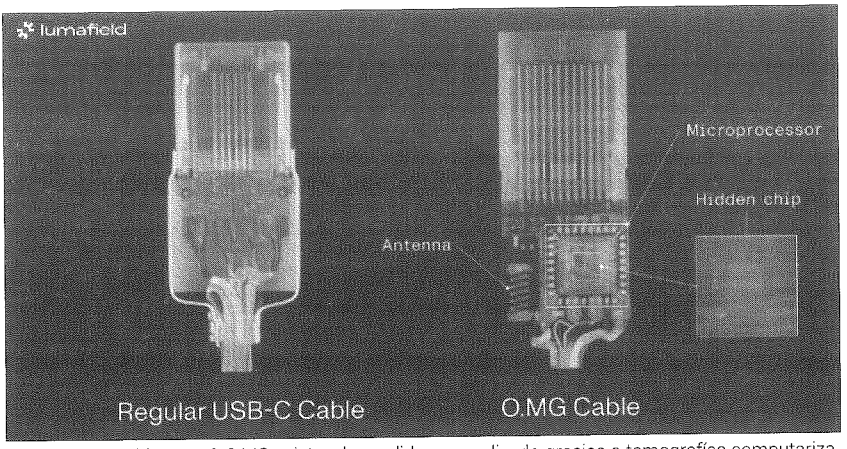


Imagen 32. El cable USB-C O.MG existe y ha podido ser analizado gracias a tomografías computarizadas en 3D[871].

9.7.2.8. Obtener

Este verbo sí es propuesto tanto por el Convenio de Budapest como por la Convención de las Naciones Unidas contra la Ciberdelincuencia.

De un lado, hay quienes entienden que en esta modalidad se "adquiere para su uso en la comisión de delitos informáticos contenidos en la Ley N.º 30096"[872]. Para otro sector, se interpreta como "alcanzar o lograr algo, y se referirá al acto a través del cual un sujeto consigue la entrega de dispositivos o

871 Forbes. *This Dangerous New Charging Cable Can Hack Your iPhone*, publicado el 16 de diciembre de 2023: https://www.forbes.com/sites/zakdoffman/2023/12/16/apple-iphone-ipad-and-macbook-users-warned-not-to-use-other-peoples-charging-cables-after-new-update/
Pc World. *How to tell if your USB cable is hiding malicious hacker hardware*, publicado el 26 de febrero de 2025. https://www.pcworld.com/article/2557422/how-to-tell-if-your-usb-cable-is-hiding-malicious-hacker-hardware.html

872 Espinoza Calderón, *Delitos informáticos y nuevas modalidades delictivas*, cit., p. 103.

mecanismos para la comisión de ciberdelitos"[873]. También es definido como "conseguir u obtener estos elementos informáticos con el fin de utilizarlo para cometer algún delito informático"[874].

Considero que esta modalidad intenta cubrir un amplio abanico de conductas relevantes penalmente y que no calzarían en el resto de supuestos previamente analizados: adquirir, comprar, recibir programas o dispositivos maliciosos que no provienen del extranjero.

A modo de resumen, la definición propuesta para los verbos rectores de este delito es la siguiente:

Verbo	Definición propuesta
Diseñar	Actividad creativa que permitirá la producción de *hardware* o *software* malicioso.
Desarrollar	Creación de *software* ilegal que no requiere soporte físico (*hardware*).
Fabricar	Construcción del soporte físico, que puede incluir *firmware*.
Facilitar	Poner a disposición *hardware* o *software* malicioso, sin que existan destinatarios específicos.
Importar	Adquirir *software* o *hardware* malicioso del extranjero.
Obtener para su utilización	Adquirir *software* o *hardware* malicioso del territorio nacional.
Distribuir	Entregar *hardware* o *software* malicioso a terceros, sin que necesariamente implique una transacción económica.
Vender	Entregar datos, *hardware* o *software* maliciosos a cambio de dinero u otro beneficio económico.

Cuadro 38. Resumen de las definiciones propuestas de los verbos que integran el delito de abuso de mecanismos y dispositivos informáticos. Elaboración propia.

9.7.3. Objeto del delito: ¿mecanismos y dispositivos informáticos?

En lo que respecta al objeto del delito, la legislación peruana ha recogido algunos de los elementos previstos en el Convenio de Budapest, aunque de manera imprecisa e incompleta, lo que justifica la necesidad de una reforma normativa en este punto. Por ejemplo, incorpora categorías como programas informáticos, dispositivos, contraseñas y códigos de acceso, pero añade el término *mecanismos*, que no se encuentra presente en los instrumentos internacionales analizados y cuya ambigüedad puede generar problemas de interpretación. Asimismo, utiliza la expresión *cualquier dato*, fórmula excesivamente genérica que contrasta con la

873 Arévalo Minchola/Vega Aguilar, *Ciberdelitos. Análisis en el sistema penal*, cit., p. 375.

874 Jiménez Herrera, *Manual de derecho penal informático*, cit., p. 485.

redacción más precisa sugerida en el Convenio de Budapest: *datos informáticos similares que permitan acceder a todo o parte de un sistema informático.*

En una eventual reforma legislativa, sería recomendable que el legislador adopte la estructura propuesta por el Convenio de Budapest, actualizada por la Convención de las Naciones Unidas sobre la Ciberdelincuencia, que distingue entre:

- Dispositivos, incluidos programas informáticos.
- Datos informáticos que permitan ingresar a un sistema, como contraseñas, credenciales de acceso y firmas electrónicas.

Esta clasificación permitiría evitar confusiones terminológicas y superposiciones conceptuales presentes en la regulación vigente. En esa línea, se propondrán a continuación definiciones más precisas que contribuyan a superar dichas ambigüedades.

9.7.3.1. Mecanismos

Este elemento no se encuentra previsto en el Convenio de Budapest ni en la Convención de las Naciones Unidas contra la Ciberdelincuencia.

Según las dos primeras acepciones recogidas por la Real Academia Española, el término *mecanismo* puede referirse a: (i) el conjunto de las partes de una máquina en su disposición adecuada, o (ii) la estructura de un cuerpo natural o artificial y la combinación de sus partes constitutivas. A partir de esta última definición, se le atribuyen sinónimos como *dispositivo*, *artefacto*, *máquina* o *engranaje*. No obstante, esta equivalencia terminológica presenta serias dificultades cuando se traslada al plano técnico-informático y jurídico.

En efecto, tanto *mecanismo* como *dispositivo* han sido incorporados por el legislador peruano en el artículo 10 LDI sin que se explicite una diferenciación conceptual entre ellos. Esta acumulación de términos, que en muchos contextos resultan sinónimos, genera un problema de ambigüedad normativa y dificulta la correcta subsunción de conductas en los tipos penales correspondientes.

Para superar este problema terminológico, propongo que el término *mecanismo* sea interpretado como una categoría general o residual, destinada a abarcar todas aquellas herramientas o estructuras funcionales orientadas a la comisión de delitos informáticos que no encajen específicamente en las nocio-

nes de *dispositivo*, *programa informático*, *dato*, *contraseña* o *código de acceso*. Esta lectura permite evitar redundancias innecesarias y asegurar una interpretación sistemática y coherente del tipo penal.

9.7.3.2. Programas informáticos

Este elemento se encuentra previsto tanto en el Convenio de Budapest como en la Convención de las Naciones Unidas contra la Ciberdelincuencia.

Los *programas informáticos* o *software* "constituyen toda secuencia de instrucciones o indicaciones destinadas a ser utilizadas, directa o indirectamente, en un sistema informático para realizar una función o una tarea o para obtener un resultado determinado, cualquiera que fuere su forma de expresión y fijación"[875].

Al estar vinculado a actividades ilícitas, nos encontraremos frente a *malwares* o programas informáticos maliciosos.

9.7.3.3. Dispositivos

Este elemento se encuentra previsto tanto en el Convenio de Budapest como en la Convención de las Naciones Unidas contra la Ciberdelincuencia.

En palabras del profesor argentino Gustavo Sain, un dispositivo informático es "un aparato capaz de procesar en forma automática datos e información con un fin determinado. El mismo debe contar con la capacidad de desempeñar tres tareas básicas, a saber: la entrada, el procesamiento y la salida de información en forma electrónica. Así, computadoras personales (PC, *notebooks*, *tablets*), teléfonos celulares, cámaras fotográficas, filmadoras, televisores inteligentes, consolas de juegos, entre otros, entran en la categoría de dispositivos informáticos"[876].

Desde esta perspectiva, los dispositivos informáticos se caracterizan por ser objetos físicos diseñados para ejecutar funciones computacionales, y se distinguen de otras herramientas informáticas -como los programas- por su naturaleza tangible y por incluir, generalmente, algún tipo de *software* embebido

875 Barrio Andrés, *Delitos 2.0. Aspectos penales, procesales y de seguridad de los ciberdelitos*, cit., p. 111.

876 Sain/Azzolin, *Delitos informáticos. Investigación criminal, marco legal y peritaje*, cit., p. 1.

(*firmware*), indispensable para su funcionamiento automático. Este componente lógico permite que el *hardware* interactúe con el entorno y realice las tareas para las que fue diseñado.

9.7.3.4. Contraseñas

Este elemento se encuentra previsto tanto en el Convenio de Budapest como en la Convención de las Naciones Unidas contra la Ciberdelincuencia.

Es toda medida de seguridad que puede ser textual -letras, números o caracteres especiales- o no textual -patrón o dibujo-, configurable por el propio usuario.

9.7.3.5. Códigos de acceso

Este elemento se encuentra previsto en el Convenio de Budapest; sin embargo, en la Convención de las Naciones Unidas contra la Ciberdelincuencia se emplea la expresión *credenciales de acceso*.

Es toda medida de seguridad que, generalmente, incluye únicamente números que no pueden ser modificados por el usuario. Por ejemplo, el CVV (*card verification value*) de las tarjetas de crédito o los códigos OTP (*one time password*) como los *tokens*.

Sobre mi propuesta, debo precisar que propongo diferenciar ambos términos según el usuario pueda o no modificarlo:

- La secuencia de tres o cuatro dígitos ubicada en la parte posterior de la tarjeta de crédito es generada por la propia entidad financiera y no puede ser modificada por el usuario. En la misma línea, la secuencia de cuatro o seis números que son enviados al llavero *token* o al celular para validar el ingreso (OTP) también es generada por el sistema y enviada temporalmente al usuario. Por esta razón, las incluyo como códigos de acceso.
- En cambio, la secuencia de números, letras o caracteres que se deben digitar para ingresar a un correo electrónico, a la intranet, al celular o a una página web las considero como contraseñas, en tanto pueden ser modificadas por el propio usuario.

- No considero adecuado diferenciarlo según sus caracteres: letras o números, pues algunos combinan ambos tipos. Además, no tendría sentido técnico considerar que una secuencia que incluye únicamente números integra la misma categoría que el *token*, pero que no se equiparan a la secuencia que incluye letras.
- Tampoco considero adecuado diferenciar ambos conceptos en función de su temporalidad. Es cierto que algunos usuarios cambian sus contraseñas con frecuencia, mientras que otros las mantienen inalteradas durante largos períodos. Por su parte, el CVV es un dato estático, en tanto que los *tokens* tienen una duración de apenas unos segundos. Sin embargo, pese a esa diferencia temporal, ambos comparten una característica esencial: no son configurables por el usuario. Esta similitud funcional los aproxima más entre sí que con las contraseñas generadas libremente por el titular. Por ello, la temporalidad no constituye un criterio válido para distinguir entre contraseñas y códigos de acceso.

9.7.3.6. Cualquier otro dato informático

Debemos recordar que las medidas de seguridad que protegen a los sistemas informáticos pueden clasificarse en tres categorías: (i) lo que tenemos -por ejemplo, una tarjeta inteligente que nos permite ingresar a un edificio o a un sistema-, (ii) lo que sabemos-como las contraseñas y los códigos de acceso-, y (iii) lo que somos -datos biométricos-.

Dicho esto, *cualquier otro dato informático* debe entenderse como cualquier representación de información biométrica que nos permite ingresar a un sistema o realizar la acción deseada por el usuario. Entre las medidas de seguridad biométrica tenemos:

- Reconocimiento facial
- Reconocimiento de iris
- Reconocimiento de retina
- Reconocimiento dactilar
- Reconocimiento de voz

Esta definición descansa en la premisa que el elemento *mecanismo* es la cláusula general de este delito. Si el legislador no lo hubiese incluido, sería este el elemento residual.

Es importante precisar que la legislación peruana ha utilizado una fórmula muy amplia al incluir este elemento (*cualquier otro dato informático*), cuando lo correcto sería delimitarlo, según ha sido propuesto tanto por el Convenio de Budapest (*datos similares que permitan acceder a todo o parte de un sistema informático*) como la Convención de las Naciones Unidas contra la Ciberdelincuencia (*datos similares mediante los cuales se pueda acceder a la totalidad o una parte de un sistema de tecnología de la información y las comunicaciones*).

Como he sostenido en capítulos anteriores, una eventual modificación debería limitar sus alcances únicamente a los delitos contra la seguridad informática y no ampliarlo a cualquier delito previsto en la LDI[877].

Objetos delictivos	Definición propuesta
Mecanismos	Elemento subsidiario que puede incluir tanto *hardware*, *software* o datos que no se subsumen en el resto de las definiciones.
Programas informáticos	Secuencia de instrucciones informáticas, conocida como *software*.
Dispositivos	Objeto físico diseñado para ejecutar una función informática.
Contraseñas	Medida de seguridad configurable por el propio usuario.
Códigos de acceso	Medida de seguridad no configurable por el propio usuario.
Cualquier otro dato informático	Representación de la información biométrica que permite realizar la acción esperada por el usuario.

Cuadro 39. Resumen de las definiciones propuestas de los objetos delictivos que integran el delito de abuso de mecanismos y dispositivos informáticos. Elaboración propia.

877 Considero que debe restringirse o limitarse el delito de abuso de dispositivos a los delitos de acceso ilícito, ataques a la integridad de datos informáticos, ataques al sistema informático e interceptación ilícita. Esto es, a los delitos que protegen la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos, tal y como lo recomienda el Convenio de Budapest e, incluso, como fue propuesto en el proyecto de Ley N.º 02520/2012: "El que fabrica, vende, facilita, distribuye u obtiene para su utilización mecanismos, dispositivos, contraseñas o códigos de acceso específicamente diseñados para la comisión de los delitos previstos en los artículos 197-A, 208-A, 208-B, 208-C y 438-A". La inadecuada ubicación y la fórmula actual origina que el abuso de dispositivos informáticos amplíe peligrosamente su utilización a delitos como el *grooming* o la suplantación de identidad.

9.7.3.7. La finalidad maliciosa como única función

El Convenio de Budapest y la Convención de las Naciones Unidas recomiendan prohibir y sancionar que los dispositivos hayan sido *concebidos o adaptados principalmente* para la comisión de cualquier delito contra la seguridad informática, es decir, diseñados o modificados, en esencia, para delinquir.

Como se puede apreciar, se propone evitar que el reproche comprenda únicamente dispositivos de una única función, sino que se incluyan los de uso dual o múltiple. No obstante, se sugiere que se castigue solo cuando la finalidad ilícita sea la principal. El debate sobre los alcances de este delito fue recogido en el Informe Explicativo, cuyo parágrafo 73 recoge lo siguiente:

> Quienes redactaron el presente Convenio debatieron largamente si el término *dispositivo* debería restringirse a aquellos diseñados exclusivamente o específicamente para cometer delitos, excluyendo en consecuencia los dispositivos que tienen un uso dual. Se consideró que este criterio era demasiado limitado. Podría dar lugar a dificultades insuperables en relación con las pruebas necesarias en un procedimiento penal, por lo que la disposición podría resultar prácticamente inaplicable o aplicable en determinadas circunstancias. También se rechazó la alternativa de incluir todos los dispositivos, incluso si son producidos y distribuidos de manera legal. En este caso, únicamente el elemento subjetivo de la intención de cometer un delito informático sería decisivo para imponer un castigo [...]. Como un compromiso razonable, el Convenio restringe su alcance a los casos en los que los dispositivos son objetivamente concebidos, o adaptados, principalmente con el fin de cometer un delito. Esto excluirá por lo general a los dispositivos de uso dual.

La redacción del actual tipo penal limita el tipo de dispositivos que originan este delito, ya que empleó una fórmula muy restrictiva y no la que sugiere el Convenio de Budapest. El artículo 10 LDI emplea la siguiente expresión: *específicamente diseñados para la comisión de los delitos previstos en la presente Ley*. Esto significa que, si nos encontramos frente a un dispositivo que no fue *específicamente* diseñado para cometer alguno de los delitos previstos en la LDI, la acción es atípica. En conclusión, la legislación peruana actual exige que se acredite que el dispositivo o mecanismo informático fue específicamente

diseñado para la comisión de un delito, lo que en la práctica equivale a requerir que su finalidad maliciosa sea única, ya que excluye otros usos legítimos.

Con la finalidad de evitar espacios de impunidad, en una eventual reforma legislativa recomiendo adoptar la fórmula recogida en España: "Concebido o adaptado principalmente para cometer dichos delitos", pero limitándolo a los delitos que atentan contra la seguridad informática.

9.8. TIPICIDAD SUBJETIVA

Nos encontramos frente a un delito doloso que, además, excluye la figura eventual al agregarse el término *deliberadamente*. De este modo, se descarta toda modalidad culposa.

En el Convenio de Budapest, en la Convención de las Naciones contra la Ciberdelincuencia y en algunas legislaciones comparadas se agrega un elemento subjetivo del injusto, añadido al dolo del autor, que se concreta con la intención específica de facilitar la comisión de ciertos delitos informáticos[878]:

> La conjunción de ambos requisitos: sin estar autorizado, más el elemento subjetivo: intención de facilitar la comisión de un delito, hace que no se castiguen, por ejemplo, la producción o adquisición de herramientas o instrumentos que si bien son aptar para cometer estos hechos ilícitos han sido creadas y comercializadas para su uso legítimo, con la autorización del titular del sistema, con el objetivo de auditar su seguridad, detectar vulnerabilidades, etc.[879].

La legislación peruana no recogió como elemento subjetivo adicional la intención del agente de facilitar la comisión de un delito informático, lo que amplía peligrosamente el rango de conductas que irracionalmente podrían ser perseguidas y castigadas. En una eventual reforma legislativa, debería incluirse el elemento bajo comentario.

878 Barrio Andrés, *Delitos 2.0. Aspectos penales, procesales y de seguridad de los ciberdelitos*, cit., p. 97. En el artículo 197 del Código Penal español, por ejemplo, se agregó el siguiente elemento subjetivo: "con la intención de facilitar la comisión de alguno de los delitos a que se refieren los apartados 1 y 2 del artículo 197 o el artículo 197 bis".

879 Gil Gil y Hernández Berlinches, *Cibercriminalidad*, cit., p. 209.

La legislación argentina tampoco lo incluye, lo que ha llevado a cierto sector de la doctrina a proponer su inclusión -con lo cual, estoy plenamente de acuerdo, ya que esto evitará criminalizar eventualmente la mera tenencia de dispositivos de doble uso-:

> Nuestro Código Penal, en el art. 183, segundo párrafo, segundo supuesto, castiga a quien vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños. El problema es que los mencionados programas, si bien pueden estar destinados a causar daños, son duales y pueden ser usados para fines loables como los mencionados sobre investigación de vulnerabilidades, *pentesting o ethical hackers*. El tipo penal argentino no pena la mera tenencia sino su distribución, introducción, uso, etc. Entendemos que lo ideal sería no poner foco en la maliciosidad del programa únicamente, como hoy lo hace la ley vigente, sino también en la intención delictiva del autor, para disminuir el espectro de punibilidad, tal como propone el Convenio de Budapest en el art. 6. En otras palabras, incorporar al tipo penal argentino una ultraintención de cometer alguno de los delitos informáticos previstos [...].
>
> En resumidas cuentas, el vigente art. 183, segundo párrafo, segundo supuesto, del Código Penal argentino no exige la demostración de ninguna ultraintención maliciosa en el autor, sino simplemente que el programa esté destinado a causar daños, con los problemas que esto podría traer para los programas con finalidades duales, conforme vimos. Por ende, respecto a los programas duales, se debe dejar abierta la posibilidad de que se pruebe el fin legítimo de su utilización, como una circunstancia eximente de responsabilidad penal, o su contracara, exigir algún tipo de intención delictiva en el autor, para que haya responsabilidad penal. Esto va en línea con el Reporte Explicativo del Convenio de Budapest[880].

880 Garat/Reale. "La reforma penal en materia de cibercrimen en la República de Argentina", cit., p. 517.

9.9. LAS SITUACIONES DE JUSTIFICACIÓN EN EL DELITO DE ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMÁTICOS

Como se ha criticado a lo largo de esta obra, no era necesario ni recomendable agregar el término *ilegítima*[881] al tipo penal. Así, incluir este innecesario elemento podría generar problemas a niveles de interpretación y de aplicación.

Ahora bien, es importante recordar que existen programas genéricos o con tecnología de doble uso, es decir, tienen más de una funcionalidad y no necesariamente será ilícita:

> Así, determinados programas denominados *keygen* (generadores de contraseña), o *cracks* (que suprimen las medidas de protección de un programa informático), pueden haber sido diseñados para varios fines, algunos de los cuales pueden resultar atípicos a todos los efectos, e incluso ilícitos, en la medida en que, por ejemplo, sean utilizados por los usuarios para realizar copias privadas de seguridad de sus propios datos, aun protegidos, conforme lo ampara la legislación sobre propiedad intelectual (art. 31 TRLPI), o bien para probar la seguridad del *software* a efectos de su certificación bajo las normas ISO. Será necesario generalmente un informe pericial para acreditar esta circunstancia[882].

Como se ha desarrollado líneas arriba, la legislación peruana excluiría estos objetos al exigir que los dispositivos y mecanismos informáticos hayan sido ***específicamente** diseñados para la comisión de los delitos previstos en la ley.*

881 En efecto, basta analizar el parágrafo 76 del Informe Explicativo para comprender que el Convenio utiliza estas expresiones para sancionar conductas dolosas y que no tienen causa de justificación: "El delito requiere que se cometa de manera deliberada e ilegítima. Con el fin de evitar el peligro de establecer demasiados delitos cuando se producen y se introducen en el mercado dispositivos para fines legítimos, por ejemplo, coma para contrarrestar los ataques contra los sistemas informáticos, se han agregado nuevos elementos para restringir el delito. Además del requisito general de que exista intención deliberada debe estar presente la intención específica es decir directa de utilizar el dispositivo para cometer cualquiera de los delitos establecidos en los artículos 2 a 5 del presente convenio".

882 Barrio Andrés, *Delitos 2.0. Aspectos penales, procesales y de seguridad de los ciberdelitos*, cit., p. 98.

[Caso 124] Juan Diego es un ingeniero informático que trabaja en la compañía Gráficas Hermanos. el gerente de tecnología de la información de la empresa, Camilo, le ha solicitado que analice los sistemas informáticos de la compañía a fin de detectar vulnerabilidades. La empresa no les ha brindado el soporte logístico necesario, razón por la cual Juan Diego y Camilo acuerdan que comprarían el *software* necesario en las galerías Wilson y así proceden. Juan Diego adquiere programas informáticos que le permiten generar contraseñas y suprimir las medidas de protección, los cuales son grabados en diversos USB. Al salir de la tienda, Juan Diego es intervenido por la policía, quienes visualizan los USB y encuentran los programas maliciosos.

En este caso, Juan Diego obtuvo para su utilización programas informáticos empleados para *hackear* y *crackear* sistemas informáticos. Desde el plano típico, el delito de abuso de mecanismos y dispositivos informáticos se encuentra plenamente configurado, sin embargo, no sería un acto ilegal, ya que operaría el artículo 20.10 CP: "El que actúa con el consentimiento válido del titular de un bien jurídico de libre disposición". De este modo, la actuación de Juan Diego se origina a pedido de quien ejerce la titularidad y cuidado del bien jurídico protegido. Ahora bien, la dificultad será de índole probatoria. Por ejemplo, ¿qué sucede si Camilo niega dicho mandato, porque no informó al gerente general o porque, en la investigación, advierte que sus facultades no le permitían adoptar tal decisión?

9.10. CONSUMACIÓN

La regulación española exige un elemento subjetivo, a diferencia de la regulación peruana, que no lo contempla. Esto es resaltado por algunos autores al analizar y sostener lo siguiente:

> El tipo penal, de mera actividad, se consuma con la acción de "producir, adquirir para usar -y no meramente poseer o detentar, como en el Art. 248.2 b) CP-, importar o facilitar a terceros" el programa espía o la contraseña ajena con la intención señalada, siendo un problema de agotamiento delictivo que se consiga o no espiar o intruir el sistema informático de otro, esto es, configurándose no como un delito de resultado, sino como uno de mero riesgo.

> Se trata de auténticos adelantamientos de la barrera de protección, en vía penal, precisamente centrados en defender las medidas de seguridad que los dispositivos tecnológicos tienen programadas por defecto, de cara a amparar cualquiera que sea la privacidad, consciente o inconsciente, que residenciemos en los constantes días de uso del mismo[883].

La doctrina nacional es clara al reconocer que nos encontramos frente a un delito de mera actividad y, en consecuencia, no admite la tentativa[884]. En efecto, este es un delito de peligro abstracto en el que se ha adelantado peligrosamente la tutela penal.

Si bien el legislador consideró necesario adelantar la barrera punitiva y, de esta forma, neutralizar aquellas conductas que podrían arriesgar la seguridad informática y otros bienes jurídicos, con la tipificación del delito de abuso de mecanismos y dispositivos informáticos, debemos diferenciar la conducta atribuida a quien provee estas herramientas del acto que realiza un tercero con aquellas.

Recordemos que existen (i) dispositivos legales que pueden ser empleados con fines ilícitos, dispositivos ilegales que pueden ser empleados únicamente con fines ilícitos y (ii) dispositivos legales que pueden ser empleados tanto con fines lícitos como ilícitos -esto es, instrumentos de doble uso-. La interpretación del artículo 10 LDI excluye la primera posibilidad, pues expresamente señala que deben haber sido diseñados específicamente para la comisión de delitos informáticos. Dicho esto, ¿podría responder a título de cómplice quien facilite herramientas diseñadas con fines lícitos, pero que son empleadas en actividades ilícitas?

En aquellos casos en los que se proporcionan herramientas informáticas lícitas, pero que son utilizadas con fines delictivos, podemos afirmar -en principio- que estamos ante una conducta neutra o estereotipada. Sin embargo,

---

883 Velasco Núñez, *Delitos tecnológicos. Cuestiones penales y procesales*, cit., p. 249.

884 Arévalo Minchola/Vega Aguilar, *Ciberdelitos. Análisis en el sistema penal*, cit., p. 380. En el mismo sentido, Meneses Gonzáles/Meneses Ochoa, *La cibercriminalidad: consideración criminológica, político-criminal, dogmática, procesal y cooperación internacional*, cit., p. 338.

existirán situaciones en las que el partícipe sí responderá penalmente como cómplice del delito imputado al autor:

> El término de "conductas neutras" de participación se aplica a aquellos comportamientos de terceros que favorecen la conducta del autor de modo estandarizado o estereotipado -en los estrictos términos de una posición social o profesional ilícita-. De modo general, cabe afirmar que se trata de casos de producción de bienes o la prestación de servicios susceptibles de un uso ilícito, pero también de uno ilícito. Por ejemplo, **la provisión de servicios de internet o la venta de componentes informáticos**, pero también de un cuchillo o de un raticida. Como se indicó, esta construcción ha sido aceptada en las últimas décadas, con más o menos matices, por la doctrina y la jurisprudencia españolas e iberoamericanas [...] En cualquier caso, la calificación de una conducta como neutra requiere que no se realicen actos de adaptación de aquella al contexto de la conducta delictiva cuya realización se favorece. En efecto, un comportamiento de favorecimiento deja de ser estandarizado tan pronto como al realizarlo se tiene en cuenta las concretas necesidades del autor o las especificidades del hecho. Así las cosas, la doctrina mayoritaria sostiene una variante objetivo-subjetiva de este planteamiento. De acuerdo con ella, se debe analizar si la conducta favorecedora muestra, en el caso concreto una inequívoca "referencia de sentido delictiva". Es decir, que carece de cualquier sentido ilícito para quien recibe el bien o el servicio. Si esta situación es, además, abarcada con dolo directo por quien realiza la conducta favorecedora, entonces su realización constituye cooperación punible. Por el contrario, en el resto de las conductas, aun realizadas con el dolo directo y, en todo caso, en las realizadas con dolo eventual, la conducta no es punible, por la vigencia del principio de confianza[885] [El resaltado es mío].

Coincido con el profesor García Cavero, quien señala que la incriminación de actos preparatorios en los delitos económicos solo se podrá legitimar de manera excepcional, si la conducta posee una univocidad lesiva en relación con

885 Silva Sánchez, *Derecho penal. Parte general*, cit., p. 1262.

intereses colectivos y, en consecuencia, desestabiliza la vigencia de la norma[886]. Este razonamiento es transferible al caso de los delitos informáticos analizados en esta obra.

9.11. CONCURSOS

Recordemos que nos encontramos frente a un delito de peligro que anticipa la tutela penal. De este modo, si el agente inicia la actuación ejecutiva de los delitos previstos en la LDI, este ilícito quedará absorbido en virtud del principio de consunción[887]. En la misma línea:

> En caso de que el mismo sujeto que produce, adquiere, importa o facilita los programas maliciosos intervenga después en los daños cometidos con dichos programas, nos encontramos ante una progresión delictiva que deberá resolverse conforme a la regla del concurso de las leyes según la cual los actos posteriores consumen a los preparatorios[888].

9.12. PENALIDAD

La sanción debe ser revisada, pues, como se ha dicho, nos encontramos frente a un delito hiperanticipado, pero que se castiga con no menos de uno ni más de cuatro años de pena privativa de libertad y con treinta a noventa días multa. Esta sanción es la misma que recibe quien comete la primera modalidad del delito de acceso ilícito, esto es, el ingreso a un sistema informático sin quebrantamiento de medidas de seguridad. No resulta adecuado castigar a quien

886 El profesor plantea como ejemplo la fabricación o posesión de instrumentos o insumos destinados a la falsificación de dinero (art. 255 CP) y precisa que "no hay duda de que el acto lesivo se produce en el momento en que se pone en circulación el dinero falsificado, pero la posesión de instrumentos o insumos destinados inequívocamente a la falsificación del dinero producen ya una perturbación social externa que defrauda la norma y que, por lo tanto, autoriza que se recurra a un restablecimiento punitivo" (García Cavero, *Derecho penal económico. Parte general*, cit., p. 693).

887 Principio de consunción: se aplica cando la sanción prevista en una ley penal engloba el supuesto de hecho de otra ley penal bajo la lógica de un solo suceso conjunto. En tal caso, la ley penal que consume el supuesto de hecho de la ley consumida desplaza a esta última en su aplicación: *lex consumens derogat legi consumptae* (Casación N.º 305-2021, Lambayeque del 23 de junio del 2022, emitida por la Sala Penal Permanente de la Corte Suprema de Justicia).

888 Gil Gil, "Daños informáticos", cit., p. 505.

obtiene un dispositivo informático destinado al *hacking* con la misma pena que recibirá quien, finalmente, accede a este[889].

La segunda parte del artículo 10 LDI sanciona a quien "[...] ofrece o presta servicio que contribuya a este propósito", es decir, a la perpetración del delito de abuso de dispositivos informáticos. Como se advierte, el primer verbo rector es *ofrecer* y ahí se presenta el problema de orden constitucional, pues, si bien es adecuado anticiparse y sancionar conductas potencialmente peligrosas, lo cierto es que este extremo anticipa demasiado la barrera punitiva estatal sin que se ponga en peligro el bien jurídico protegido.

Por otro lado, la expresión *prestar servicio* resulta innecesaria y carece de relación con la propuesta recogida en el Convenio de Budapest. Este problema surge porque el legislador incorporó la modalidad prevista en el artículo 6 del proyecto de Ley N.º 34/2011, el cual no contemplaba las diversas conductas sugeridas en dicho convenio. En contraste, estas sí estaban incluidas en el proyecto de Ley N.º 2520/2011, presentado por el Ejecutivo. En otras palabras, el actual artículo 10 de la LDI es el resultado de la fusión de dos propuestas legislativas incompatibles, lo que evidencia la necesidad de una reforma normativa.

9.13. CIRCUNSTANCIAS AGRAVANTES

Son aplicables las cinco circunstancias previstas en el artículo 11 de la Ley N.º 30096:

i) Cometer el delito como integrante de una organización criminal.

ii) Cometer el delito mediante el abuso de una posición especial de acceso a la data o información reservada o al conocimiento de esta información en razón del ejercicio de un cargo o función.

iii) Cometer el delito con la finalidad de obtener un beneficio económico.

iv) Comprometer fines asistenciales, la defensa, la seguridad y la soberanía nacionales.

889 Siguiendo la línea crítica, Aboso (*Derecho penal cibernético: La cibercriminalidad y el derecho penal en la moderna sociedad de la información y la tecnología de la comunicación*, cit., p. 366).

v) Cometer el delito empleando la inteligencia artificial o tecnologías similares o análogas (conforme a la Ley N.º 32314).

9.14. PROPUESTA NORMATIVA

A partir del análisis expuesto en este capítulo, propongo modificar el delito de abuso de dispositivos y mecanismos informáticos, tomando en consideración:

i. Reformar el *nomen iuris* del delito actualmente denominado *abuso de mecanismos y dispositivos informáticos*, sustituyéndolo por *abuso de dispositivos informáticos*.

ii. Eliminar los elementos *deliberada* e *ilegítimamente*.

iii. Eliminar el elemento *mecanismos* del tipo penal, al ser una expresión imprecisa desde el plano técnico jurídico.

iv. Eliminar el verbo *diseñar* del tipo penal, por ser una conducta hiperanticipada.

v. Unir los verbos *fabricar* y *desarrollar* en el verbo *producir* -recomendado por el Convenio de Budapest y la Convención de las Naciones Unidas contra la Ciberdelincuencia-.

vi. Reemplazar el verbo *facilitar* por *poner a disposición*.

vii. Modificar los alcances de delito, reemplazando la expresión *delitos previstos en la presente Ley*, por la expresión *delitos previstos en los artículos 2, 3, 4 y 7 de la presente ley*.

viii. Eliminar la segunda modalidad recogida en la actual norma, esto es, *ofrecer o prestar servicio que contribuya a este propósito*.

ix. El delito debe ser reubicado en el capítulo de "Delitos contra la seguridad informática" o "Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas".

x. Modificar el rango de la sanción penal.

De este modo, el delito bajo estudio se regularía en los siguientes términos:

Art. 10.- Abuso de dispositivos informáticos

Será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa, el que, con

la finalidad de cometer los delitos en los artículos 2, 3, 4 y 7 de la presente ley, importa, produce, distribuye, vende, pone a disposición u obtiene para su utilización:

1. Dispositivos o programas informáticos, concebidos o adoptados para cometer dichos delitos;
2. Contraseñas, códigos de acceso o cualquier otro dato informático que permitan acceder a todo o parte de un sistema informático.

9.15. CONCLUSIONES DEL CAPÍTULO

- La redacción actual del artículo 10 de la LDI amplía injustificadamente los alcances del tipo penal al sancionar conductas relacionadas con mecanismos y dispositivos informáticos sin circunscribirlas únicamente a los delitos que afectan la confidencialidad, integridad y disponibilidad de los sistemas. Esta ampliación entra en tensión con el principio de lesividad y debilita la seguridad jurídica, ya que convierte en delictivas conductas que podrían no representar un riesgo real para los bienes jurídicos protegidos por el derecho penal informático. En ese sentido, es necesario replantear su alcance y adecuarlo a los estándares internacionales que han delimitado de forma más precisa este delito.
- El capítulo demuestra que la ubicación normativa del delito de abuso de mecanismos y dispositivos informáticos en una sección genérica ha contribuido a la confusión sobre el bien jurídico protegido. A diferencia de la lógica seguida por el Convenio de Budapest y la Convención de las Naciones Unidas, la ley peruana no vincula este delito exclusivamente con la protección de la seguridad informática, lo cual debilita la coherencia del sistema penal y genera ambigüedad en su interpretación. Se recomienda, por tanto, redefinir su ubicación dentro de la LDI y afirmar su naturaleza como delito de peligro orientado a tutelar un bien jurídico único: la seguridad informática.
- Una de las críticas más relevantes formuladas en este capítulo es la inclusión del verbo rector *diseñar*, que corresponde a una etapa preliminar del ciclo de vida de un programa o dispositivo, muchas veces desvinculada de un riesgo concreto. Al criminalizar actos de

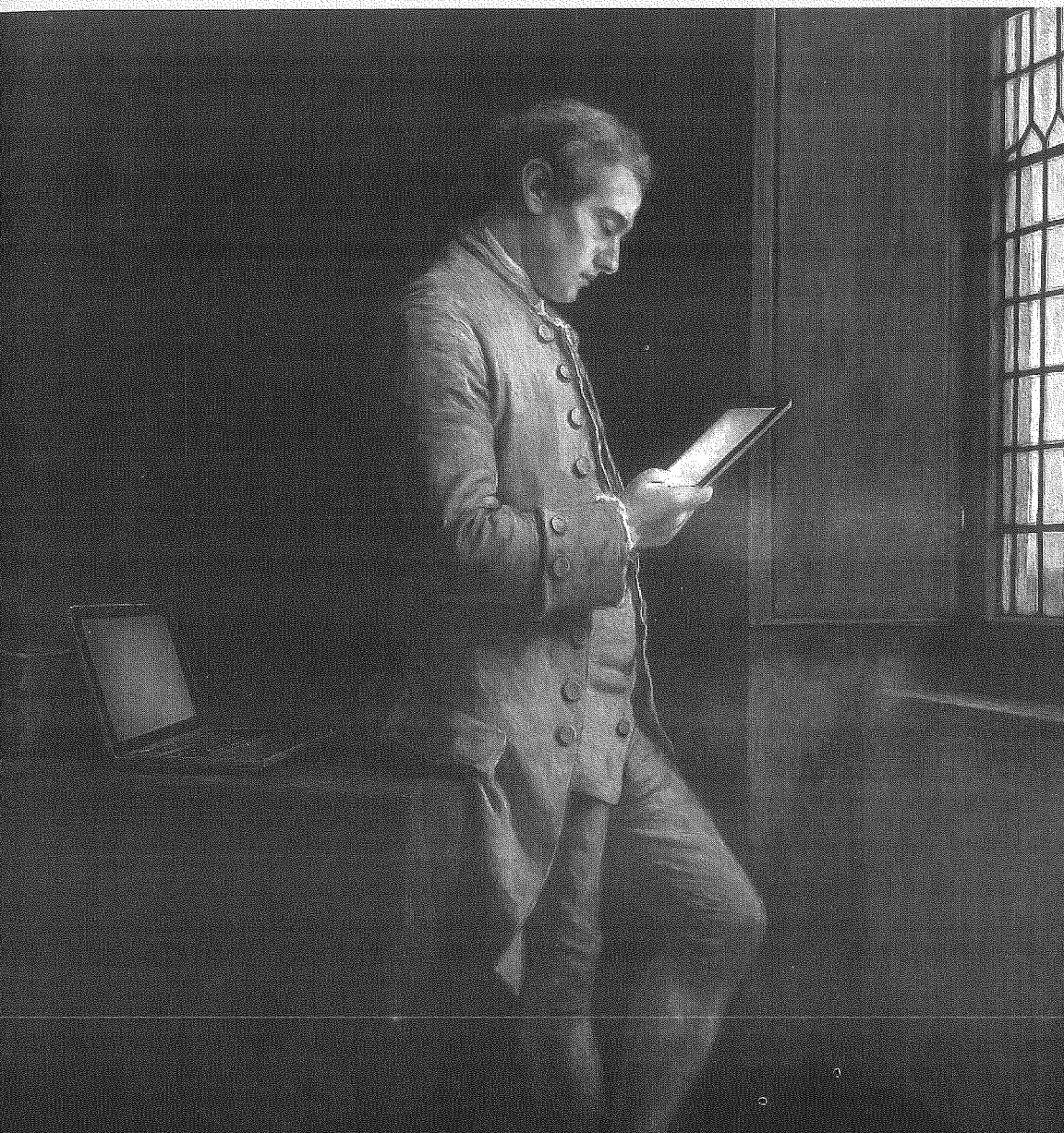
mera planificación o diseño sin exigencias de vinculación objetiva con un uso delictivo, se pone en cuestión la proporcionalidad y necesidad de la intervención penal. Tal formulación puede derivar en una expansión punitiva injustificada.

- El Convenio de Budapest y la Convención de las Naciones Unidas contra la Ciberdelincuencia proporcionan un marco técnico-jurídico más depurado y garantista, al delimitar el tipo penal a la producción, venta, obtención para su utilización, importación, difusión u otra puesta a disposición de dispositivos específicamente destinados a cometer ciertos delitos contra la seguridad informática.
- Aunque se pretende reforzar el elemento subjetivo del delito mediante la inclusión de la fórmula *deliberada* e *ilegítimamente*, esta redacción no aporta claridad ni precisión. La doctrina y legislación comparada muestran que no es necesario incorporar estas expresiones para dejar constancia del carácter doloso del delito. Su inclusión, por el contrario, puede dificultar la subsunción normativa e introducir ambigüedades que comprometan la técnica legislativa. Se recomienda eliminar ambos términos al devenir en innecesarios.
- La reserva formulada por Perú frente al artículo 6, párrafo 1, literal b del Convenio de Budapest -referida a la posesión de dispositivos para fines delictivos- resulta razonable desde el punto de vista político-criminal. La prueba del elemento subjetivo que acompaña a la posesión es particularmente compleja, ya que no basta la tenencia material del dispositivo, sino que debe demostrarse su finalidad delictiva. Esta carga probatoria puede generar arbitrariedades y falsear el equilibrio procesal, por lo que es prudente mantener esta exclusión en la legislación vigente.
- En este capítulo se evidencia cómo la actual redacción del tipo penal incluye conductas que no necesariamente representan una amenaza concreta a la seguridad informática, como el ofrecimiento o la prestación de servicios, incluso cuando estos no han llegado a ejecutarse ni a generar un riesgo inminente. Una reforma legislativa debería eliminar esta modalidad, ajustándose a una visión restrictiva y proporcionada del derecho penal.

- La comparación con otras legislaciones latinoamericanas demuestra que Perú ha adoptado un enfoque aislado, tanto en la selección de los verbos rectores como en la identificación de los objetos materiales del delito. Mientras que otros países se limitan a castigar conductas claramente vinculadas con herramientas maliciosas, la legislación peruana incorpora términos vagos como *mecanismos* o *cualquier otro dato informático*, lo que incrementa la inseguridad jurídica. Una revisión técnica del tipo penal debe considerar estos contrastes y buscar una armonización con las mejores prácticas regionales e internacionales.
- El hecho de que el delito haya sido ubicado en el capítulo de "Disposiciones comunes", junto a los artículos sobre agravantes y exenciones, impide su adecuada sistematización dentro del conjunto de delitos informáticos. Esta elección legislativa contradice su naturaleza como figura de protección anticipada frente a amenazas concretas contra la seguridad informática. Por ello, se recomienda reubicar este delito junto a los de acceso ilícito, atentados contra datos y sistemas informáticos e interceptación de datos, de modo que se refuerce su función preventiva y su conexión con el núcleo del bien jurídico protegido.
- El análisis del tipo penal pone en evidencia la necesidad de una reforma que respete el principio de proporcionalidad, delimite de manera precisa los objetos materiales ilícitos y defina con claridad las conductas típicas reprochables. Esta reforma debe evitar redundancias y suprimir verbos innecesarios. Solo así se garantizará una adecuada armonía entre la eficacia de la norma penal y el respeto por los derechos fundamentales.

CAPÍTULO 10

ESTUDIO DE PROYECTOS DE LEY RELACIONADOS A LOS CIBERDELITOS CONTRA LA SEGURIDAD INFORMÁTICA



* La ilustración de la página anterior corresponde a una adaptación de *The Reader in White*, de Jean Louis Ernest Meissonier (1857). Para su elaboración, se empleó una de las herramientas de generación de imágenes de la empresa OpenAI.

CAPÍTULO 10

ESTUDIO DE PROYECTOS DE LEY RELACIONADOS A LOS CIBERDELITOS CONTRA LA SEGURIDAD INFORMÁTICA

Sumario: 10.1. Introducción. 10.2. PL N.º 5071/1999-CR. 10.3. PL N.º 5132/1999-CR. 10.4. PL N.º 1744/2000. 10.5 PL N.º 2226/2002-CR. 10.6. PL N.º 7197/2003-CR. 10.7. PL N.º 10079/2003-CR. 10.8. PL N.º 11346/2004-CR. 10.9. PL N.º 11402/2004-CR. 10.10. PL N.º 1318/2006-CR. 10.11. PL N.º 1828/2007-CR. 10.12. PL N.º 3083/2008-CR. 10.13. PL N.º 4279/2010-CR. 10.14 PL N.º 34/2011-CR. 10.15 PL N.º 307/2011-CR. 10.16. PL N.º 1136/2011-CR. 10.17. PL N.º 1257/2011-CR. 10.18. PL N.º 2129/2012-CR. 10.19 PL N.º 2520/2012-PE. 10.20. PL N.º 2991/2013-CR. 10.21. PL N.º 2999/2013-CR. 10.22 PL N.º 3105/2013-CR 10.23 PL N.º 3980/2014-CR. 10.24. PL N.º 5630/2020-CR. 10.25 PL N.º 9136/2024-CR. 10.26. PL N.º 9443/2024-CR.

La pregunta central, sin importar el papel que desempeñes en ciberseguridad, es la siguiente: "¿Por qué las personas se comportan de la manera que lo hacen?". La identidad, la experiencia vivida, la cultura, la comunidad, las normas sociales y otros factores influyen en el comportamiento de individuos e instituciones y, en consecuencia, en la forma en que usan la tecnología, perciben el riesgo y adoptan medidas para mitigarlo mediante seguridad y privacidad. Las personas introducen su perspectiva personal e inevitablemente sesgos de todo tipo en la creación, adopción, implementación y uso de tecnología. Esa es la psicología básica. Por lo tanto, como profesional de la seguridad de la información, las técnicas y políticas que implementes para combatir las amenazas a la seguridad de la información deben tener en cuenta el elemento humano, lo que incluye reconocer cómo el sesgo cognitivo afecta a tu toma de decisiones[890].

890 Stewart, Camille. "Mantener a las personas en el foco del problema". En: Morillo, Christina (ed.). *97 cosas que todo profesional de la seguridad informática debería saber.* Madrid: Grupo Anaya, 2022, p. 39.

10.1. INTRODUCCIÓN

El objetivo de este capítulo será que el lector cuente con herramientas de análisis complementarias que le permitan identificar núcleos problemáticos que subsisten hoy en día y, quizás, revalorar algunas fórmulas legislativas que permitirían investigar y sancionar ciertas conductas delictivas de manera mucho más eficaz.

El estudio del proceso legislativo ha sido analizado y abordado por el profesor Manuel Atienza, de cuya obra extraigo las siguientes reflexiones:

> Se ha dicho ya que la técnica legislativa se plantea como objetivo la optimización de la producción de las leyes, y la teoría de la legislación, la explicación del fenómeno de la legislación desde una perspectiva general. Pues bien, el proceso de producción de las leyes -la legislación- puede verse como una serie de interacciones que tienen lugar entre elementos distintos: edictores [sic], destinatarios, sistema jurídico, fines y valores. Desde una perspectiva muy abstracta, puede decirse que los edictores [sic] son los autores de las normas; los destinatarios, aquellos a quienes estas se dirigen; el sistema jurídico, el conjunto del que pasa a formar parte la nueva ley; los fines, los objetivos o metas (entendidos en el sentido más amplio) que se persiguen al establecer las leyes; y los valores, las ideas que sirven para justificar dichos fines. El producto de tales interacciones son las leyes. Estas constituyen, al mismo tiempo, el punto de partida para nuevos procesos (la interpretación y aplicación) en los que se centra la dogmática si se desea comprender, e intervenir en la producción legislativa.
>
> Ahora bien, en el análisis del fenómeno de la legislación no están solamente implicadas las disciplinas jurídicas de corte más o menos tradicional (a la dogmática jurídica habría que añadir, obviamente, el Derecho comparado y la teoría general del Derecho), sino también conocimientos de tipo formal (como la lógica o la informática), prácticamente todas las disciplinas humanas y sociales (de manera destacada, ciencias del lenguaje y la sociología) y la propia filosofía. Por otro lado, el discurso sobre la legislación que se presenta bajo el rótulo de "ciencia", "doctrina", "teoría", "técnica", etc., suele ser, de hecho, heterogéneo, en cuanto que pretende cumplir una pluralidad de funciones: no

> solo describir la actividad legislativa, sino también explicarla, criticarla y proponer medidas para mejora[891].

De este modo, en este capítulo analizaré diversos proyectos de ley relacionados únicamente al acceso ilícito, ataques contra la integridad de los datos y sistemas informáticos, interceptación ilegal de datos y abuso de mecanismos y dispositivos informáticos. El lector encontrará cada fórmula legislativa propuesta y su respectiva exposición de motivos, lo que, por su alto valor académico, permite comprender el contexto[892] que subyace a cada propuesta normativa, así como el origen de algunos problemas de tipificación y sistematización -que, en cierta medida, han sido abordados en los capítulos precedentes-. Es más, algunos proyectos recogen estadística valiosa que permite reconstruir el avance del fenómeno delictivo y que no ha sido recogido por otras entidades gubernamentales.

Toda vez que este libro aborda la ciberdelincuencia pura, en este espacio no abordaré otros delitos ni fórmulas procesales recogidos en los proyectos de

---

891 Atienza, Manuel. *Argumentación legislativa*. Buenos Aires: Astrea, 2019, pp. 8 y 9.

892 No pretendo que el lector abrace el *método histórico* de interpretación normativa, pues su utilización es muy discutida, sino que, con fines académicos y de investigación, nos transportemos a los años en los que se advertía la necesidad de contar con un cuerpo legislativo robusto para enfrentar un fenómeno criminal que se encontraba en aumento. Sobre el referido cuestionamiento, el profesor Marcial Rubio Correa destaca que este método "puede aportar elementos de juicio interesantes en la interpretación, pero su uso es muy discutido porque muchas veces la intención del legislador no es manifiesta; otras es determinada con mucho contenido subjetivo por el intérprete y otras, finalmente, el resultado de la interpretación histórica es un obstáculo a la necesaria adaptación del Derecho a las nuevas circunstancias sociales a las que pretende normar" (Rubio Correa, *El sistema jurídico. Introducción al derecho*, cit., p. 273). En la misma línea de cuestionamientos, David Martínez Zorrilla, precisa que el argumento psicológico o de la voluntad del legislador "consiste en intentar fundamentar la interpretación de la disposición en aquello que pretendía o entendía la autoridad concreta que la dictó [...]. Este argumento puede resultar persuasivo, porque se presenta como el más respetuoso con el legislador, el que más se somete a su autoridad y el que menor margen de maniobra deja a la tarea creativa de los jueces y demás intérpretes. Con todo, presenta importantes problemas, tanto desde una perspectiva epistemológica (conocimiento) como justificativa" (Martínez Zorrilla, David. *Metodología jurídica y argumentación*. Madrid: Marcial Pons, 2010, p. 74).

ley -lo cual, incluso, ha sido omitido en la transcripción para evitar cualquier confusión-.

10.2. PROYECTO DE LEY N.º 5071/99-CR, LEY DE DELITOS INFORMÁTICOS

Fecha de presentación: 18 de agosto de 1999

Congresista proponente: Jorge Muñiz Ziches

10.2.1. Fórmula legal

Ley de Delitos Informáticos

Artículo único.- Incorpórese al Código Penal, promulgado por Decreto Legislativo N.º 635, el Capítulo XI, Delitos Informáticos, los artículos 208a y 208b, con los siguientes textos:

Artículo 208a.- El que indebidamente utilice o ingrese a una base de datos, sistema o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio con el fin de defraudar, obtener dinero, bienes o información será reprimido con pena privativa de libertad no mayor de dos años, o con prestación de servicios comunitario de cincuentidós [sic] a ciento cuatro jornadas.

Artículo 208b.- El que indebidamente, interfiere, recibe, utilice, altere, dañe o destruya un soporte o programa de computadora o los datos contenidos en la misma, en la base, sistema o red será reprimido con pena privativa de libertad no mayor de dos años.

10.2.2. Exposición de motivos

Véase el texto completo de esta exposición de motivos en el siguiente enlace:



10.2.3. Comentarios

La historia de la ciberdelincuencia en el Perú recuerda este como el primer proyecto de ley que propuso incorporar los ciberdelitos puros o atentados

contra la seguridad informática al Código Penal. El lector debe recordar que, en aquella época, ni siquiera se había aprobado el Convenio de Budapest, razón por la cual la fórmula legislativa no emplea los verbos rectores sugeridos en el citado instrumento.

Como se ha dicho líneas arriba, el legislador propuso incluir este delito como capítulo XI, esto es, en el título que recoge los delitos contra el patrimonio, lo que, finalmente, sucedió. Hoy sabemos que esta modalidad de ciberdelincuencia no tiene como objeto de protección el patrimonio, sino otros bienes jurídicos: la seguridad informática o, según otras posiciones, la integridad de los datos y sistemas, la intimidad, la privacidad, etc.

Tan incipiente fue la discusión inicial que el legislador tuvo que precisar en la exposición de motivos que "los llamados delitos informáticos no son cometidos por la computadora, sino que es el hombre quien los comete con ayuda de aquella". Actualmente discutimos sobre el uso de la inteligencia artificial como herramienta de asistencia para la comisión de delitos informáticos y tradicionales; en cambio, a fines de los noventa, el uso de las computadoras y el internet era el objeto central de preocupación.

El primer delito propuesto (art. 208.a) sancionaba el acceso ilegal, exigiendo para su configuración no solo el ingreso o empleo de un sistema informático, sino, además, un propósito ilegal -esto es, incluía un elemento subjetivo trascendente-. Dicho esto, la fórmula presentaba la siguiente estructura típica:

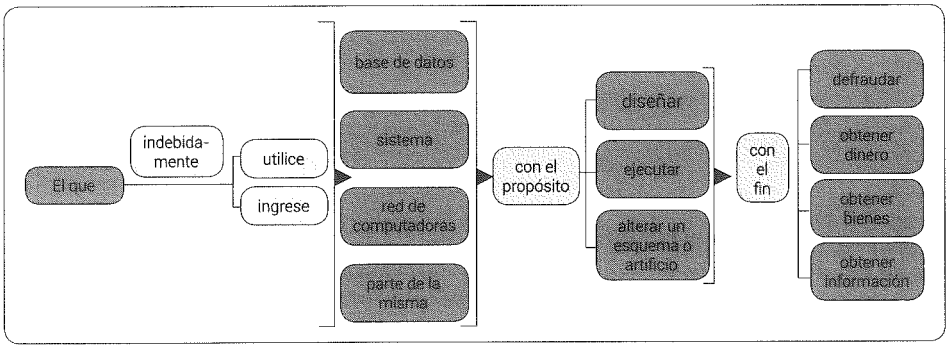


Diagrama 23. Estructura del delito de acceso ilícito, propuesto en el PL N.º 5071/99-CR. Elaboración propia.

El segundo delito propuesto (art. 208.b) sancionaba el daño y sabotaje informático, sancionando a quien de forma indebida -esto es, sin autorización-

atentaba contra un soporte, un programa de computadora o contra los datos informáticos contenidos en estos. La fórmula propuesta por el legislador puede graficarse de la siguiente forma:

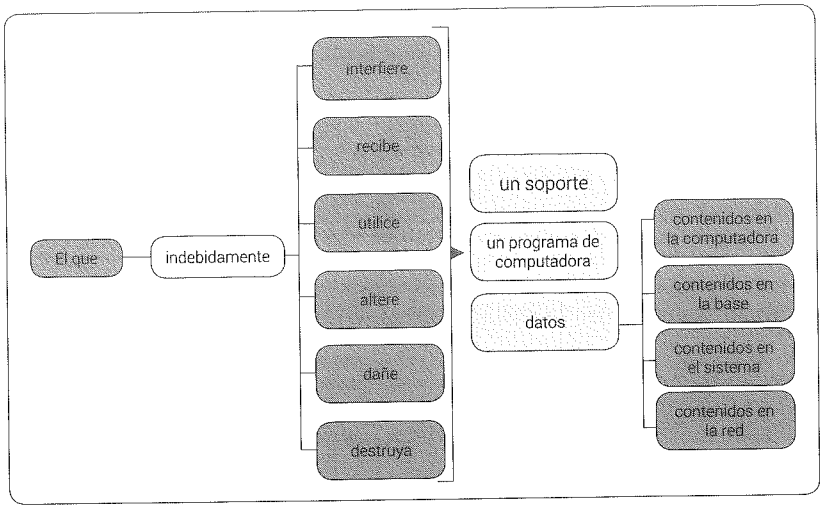


Diagrama 24. Estructura de los delitos de daños y sabotaje informático, propuestos en el PL N.° 5071/99-CR. Elaboración propia.

En esta propuesta, el legislador contemplaba una sanción leve, esto es, no más de dos años de pena privativa de libertad en ambos supuestos.

10.3. PROYECTO DE LEY N.° 5132/99-CR, LEY QUE PROPONE ESTABLECER COMO FIGURA TÍPICA PENAL LOS DELITOS INFORMÁTICOS

Fecha de presentación: 31 de agosto de 1999

Congresista proponente: Ivonne Susana Díaz Díaz

10.3.1. Fórmula legal

Ley de Delitos Informáticos

Artículo 1.- El que maliciosamente destruya o inutilice el soporte lógico de un sistema computacional, empleando medios computacionales, será reprimido con pena privativa de libertad no mayor a cuatro años.

Artículo 2.- El que con ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento

masivo de la misma, lo intercepte, lo interfiera o acceda a él, será reprimido con pena privativa de libertad no mayor de tres años.

Artículo 3.- El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema informático de tratamiento de información, será reprimido con pena privativa de libertad no mayor de cuatro años.

Artículo 4.- El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá pena privativa de libertad no mayor de cuatro años. Si quien incurre en estas conductas es el responsable del sistema de información, la pena será no mayor de seis años.

10.3.2. Considerando / Exposición de motivos

Véase el texto completo de esta exposición de motivos en el siguiente enlace:	

10.3.3. Comentarios

Este es el primer proyecto de ley que propone la creación de una ley penal especial para combatir la ciberdelincuencia. A diferencia del proyecto previamente analizado y los siguientes, que proponen incorporar los delitos al Código Penal, en este proyecto se advierte la necesidad de adoptar un marco normativo que reconozca un nuevo objeto de protección. De ahí que no recomiende incluir estos tipos penales a los delitos contra el patrimonio.

De otro lado, es interesante reconocer que esta propuesta se aproxima a la tipificación de los ciberdelitos puros -esto es, aquellos en los que se utilizan las TIC como medio y fin delictivo- y los ciberdelitos réplica -literalmente se reconoce que "ciertas figuras típicas convencionales han comenzado a realizarse mediante el empleo de la tecnología de la información, es decir, ha comenzado a ser utilizada la informática como un medio de comisión específico"-.

El primer delito propuesto es el de sabotaje informático, destacando que utiliza el término *maliciosamente* como elemento subjetivo del tipo. Si recordamos la crítica formulada a lo largo de esta obra contra el elemento *deliberadamente*, el lector establecerá que esta inclusión es innecesaria. Este ilícito remarca la naturaleza informática tanto del instrumento -medios computacionales- como

del objetivo -soporte lógico de un sistema computacional-. Finalmente, se contemplan únicamente dos tipos de acciones: destruir e inutilizar.

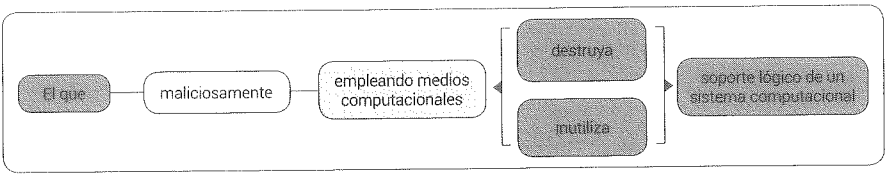


Diagrama 25. Estructura del delito de sabotaje informático, propuesto en el PL N.° 5132/99-CR. Elaboración propia.

El segundo delito reúne tanto el acceso ilícito como la interceptación ilegal de datos. En este caso, en vez de utilizar el elemento *maliciosamente*, se emplea un elemento subjetivo trascendente: el ánimo de usar o conocer información contenido en un soporte informático. En cuanto a las conductas, se sanciona la interceptación, la interferencia y el acceso ilegal.

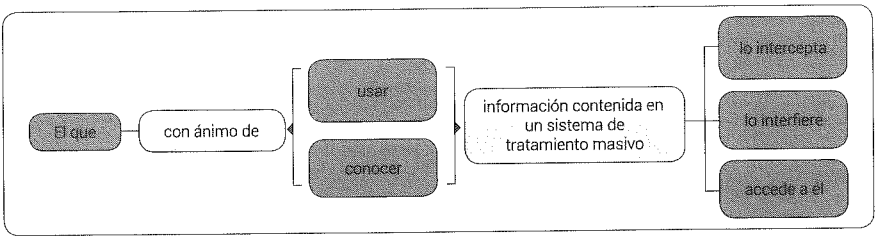


Diagrama 26. Estructura de los delitos de acceso e interceptación ilícita, propuestos en el PL N.° 5132/99-CR. Elaboración propia.

El tercer delito propuesto tipifica los daños informáticos, sancionando a quien altera, daña o destruye datos contenidos en un sistema. Es importante resaltar que en este proyecto se emplea la expresión *sistema informático* -cuyo uso sería estandarizado y difundido gracias al Convenio de Budapest-. A diferencia del sabotaje informático, propuesto en el primer artículo, no se emplea el término *inutiliza*, sino que, en su reemplazo, propone dos verbos rectores: *alterar* y *destruir* -los cuales, a la fecha, aún se siguen empleando en la LDI-.

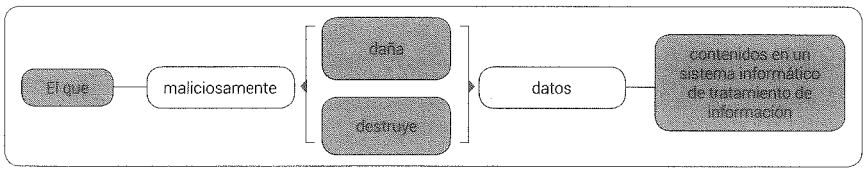


Diagrama 27. Estructura del delito de daños informáticos, propuesto en el PL N.° 5132/99-CR. Elaboración propia.

El cuarto ilícito recoge la revelación ilegal de datos informáticos, delito que no está contemplado en el Convenio de Budapest ni en la LDI. En cuanto a la estructura, es similar al delito de daños informáticos -en tanto recoge el elemento maliciosamente, así como los datos contenidos en sistemas informáticos-. En este caso, se advierte una circunstancia agravante por la condición del autor: responsable del sistema de información.

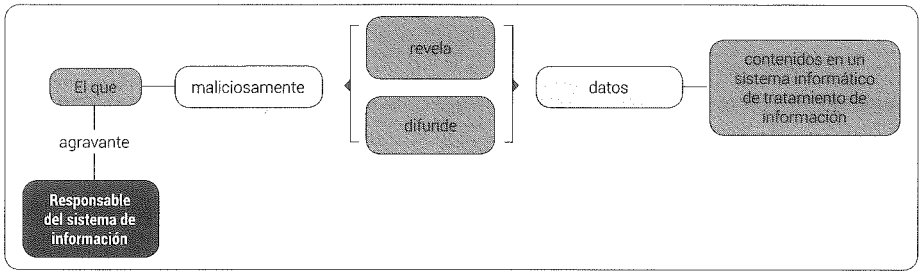


Diagrama 28. Estructura del delito de revelación de datos informáticos, propuesto en el PL N.° 5132/99-CR. Elaboración propia.

A diferencia del primer proyecto de ley analizado, las sanciones son mayores en los cuatro delitos propuestos, pues alcanzan los tres, cuatro y seis años de pena privativa de libertad.

Es importante reconocer que este proyecto de ley precisa que los delitos informáticos atentan contra el soporte lógico (*software*) y no físico (*hardware*), pues contra este último se cometen delitos tradicionales o convencionales, como los daños, por ejemplo. Esta aclaración resulta importante, pues nos permite identificar que el objeto de protección no es el cascarón, sino el contenido. Así, siguiendo la exposición de motivos, estos ilícitos serían manifestaciones de daños a datos computarizados.

El lector debe recordar que estos proyectos de ley iniciales decantaron en la promulgación de la Ley N.° 27309 del 17 de julio de 2000, norma que incorporó los delitos informáticos al Código Penal peruano.

10.4. PROYECTO DE LEY N.º 1744/2000, LEY QUE MODIFICA LOS ARTS. 207-A, 207-B Y 207-C DEL TÍTULO V DEL LIBRO II DEL CÓDIGO PENAL, DL 635 REFERENTE A LOS DELITOS INFORMÁTICOS

Fecha de presentación: 20 de abril de 2001

Congresista proponente: Rafael Castañeda Castañeda

10.4.1. Fórmula legal

Ley que modifica los art. 207-A, 207-B y 207-C, del Título V del Libro II del Código Penal, D.L. 635 referente a los delitos informáticos

Artículo 1.- Modificase el Título V del Libro II del Código Penal, promulgado por el Decreto Legislativo N.º 635, en los siguientes términos:

Capítulo X. Delitos Informáticos

Artículo 207-A.- El que utiliza o ingresa indebidamente a una base de datos, sistema o red de computadoras o cualquier parte de la misma, para diseñar, ejecutar o alterar un esquema u otro similar, o para interferir, interceptar, acceder o copiar información en tránsito o contenida en una base de datos, será reprimido con pena privativa de libertad no mayor de dos años o con prestación de servicios comunitarios de cincuentidós a ciento cuatro jornadas **e inhabilitación conforme al artículo 36, inciso 4, hasta por dos años.**

Si el agente actuó con el fin de obtener un beneficio económico, será reprimido con pena privativa de libertad no mayor de tres años o con prestación de servicios comunitarios no menor de ciento cuatro jornadas **e inhabilitación conforme al artículo 36, inciso 4, hasta por cinco años**

Artículo 207-B.- El que utiliza, ingresa o interfiere indebidamente una base de datos, sistema, red o programa de computadoras o cualquier parte de la misma con el fin de alterarlos, dañarlos o destruirlos, será reprimido con pena privativa de libertad no menor de tres un mayor de cinco años y con setenta a noventa días multa **e inhabilitación conforme al artículo 36, inciso 4, hasta por cinco años.**

Artículo 207-C.- En los casos de los artículos 207-A y 207-B, la pena será privativa de libertad no menor de cinco ni mayor de siete años, **e inhabilitación conforme al artículo 36, inciso 4,** cuando:

1. El agente accede a una base de datos, sistema o red de computadora, haciendo uso de información privilegiada, obtenida en función a su cargo.
2. El agente pone en peligro la seguridad nacional.

10.4.2. Considerando / Exposición de motivos

Véase el texto completo de esta exposición de motivos en el siguiente enlace:	

10.4.3. Comentarios

Siguiendo la tendencia de esta época, este proyecto propone incorporar los delitos informáticos al Código Penal, específicamente como un capítulo dentro del título de delitos contra el patrimonio.

Nuestro legislador consideró, de forma acertada, tipificar los delitos informáticos. Sin embargo, abogó por una política de represión, esto es, a mayor sanción, menor incidencia delictiva -cuando esta afirmación, empíricamente, no puede ser comprobada-: "Se hace necesario, por lo tanto, penalizar con mayor rigurosidad los ilícitos informáticos, por lo que se deben dictar normas penales mucho más estrictas a fin de dotar al órgano jurisdiccional de los dispositivos legales eficaces que permitan disuadir y sancionar a los infractores".

El lector, al igual que yo, habrá advertido diversas coincidencias entre esta exposición de motivos y la presentada dos años antes -por ejemplo, al explicar que los ataques contra el soporte físico configuran delitos convencionales o la tipología de delitos informáticos empleada-.

El primer delito (art. 207-A) tipifica tanto el acceso ilícito (ingresar indebidamente) como una modalidad de sabotaje informático (utilizar un sistema o similar para alterarlo). Como he indicado con anterioridad, no se utiliza un término que permita comprender todas las manifestaciones del sistema, sino que se hace referencia a diferentes manifestaciones o, incluso, a bases de datos. Se advierte también un elemento subjetivo adicional: la finalidad del acceso o de la utilización, esto es, el diseño, la ejecución, la alteración, la interferencia,

la interceptación, el acceso o el copiado de información. Además, si el agente actuó con *animus lucrandi*, la sanción se incrementa.

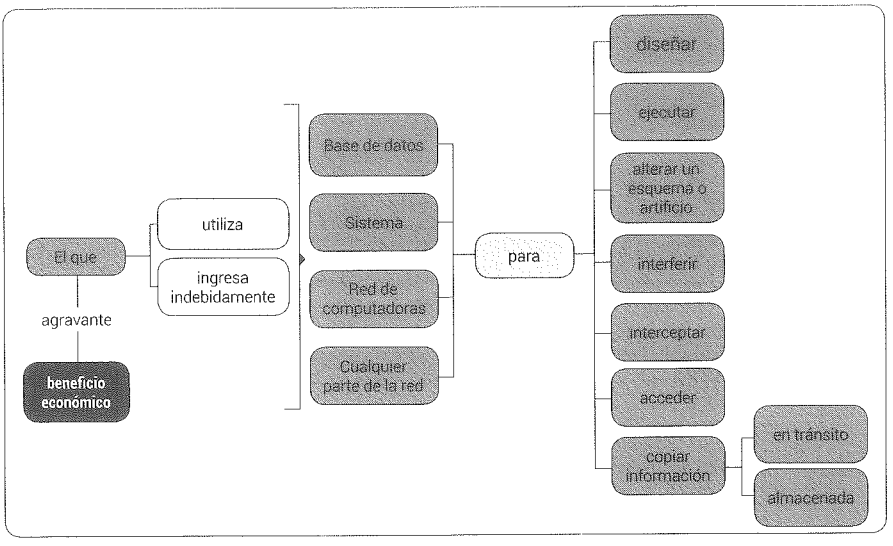


Diagrama 29. Estructura del delito de acceso ilícito y sabotaje informático (alteración), propuesto en el PL N.° 01744/2000-CR. Elaboración propia.

El segundo delito (art. 207-B) también tipifica el acceso ilícito y el sabotaje informático, pero cuando persigue la alteración, daño o destrucción del sistema informático -incluyendo los programas de computadoras, es decir, los *softwares*-. Si bien el legislador trató de diferenciar estas dos conductas, ciertamente, la redacción y propuesta son confusas, ya que solo se diferencian por la intención perseguida, lo que dificultaría su probanza.

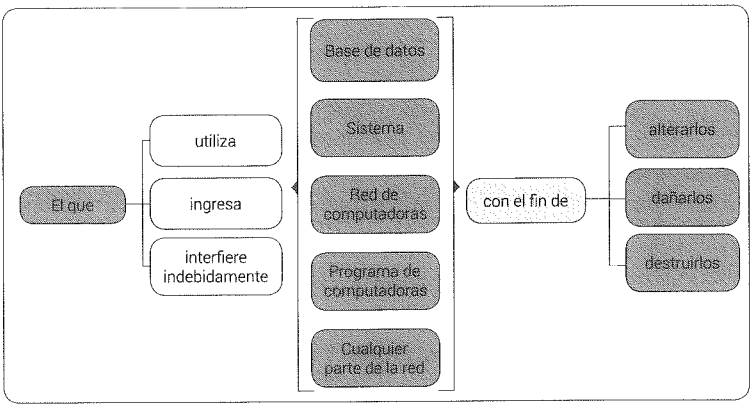


Diagrama 30. Estructura del delito de acceso ilícito y sabotaje informático (alteración, daño y destrucción), propuesto en el PL N.° 01744/2000-CR. Elaboración propia.

Finalmente, este proyecto recoge dos circunstancias agravantes: (1) hacer uso de la información privilegiada, obtenida en función al cargo del agente -los *insiders*, por ejemplo-; (2) arriesgar la seguridad nacional -es decir, por las graves consecuencias que puede generar la conducta desplegada-.

10.5. PROYECTO DE LEY N.° 2226/2002-CR, LEY QUE MODIFICA LOS ARTS. 207-A, 207-B Y 207-C DEL TÍTULO V DEL LIBRO II DEL CÓDIGO PENAL, DL 635 REFERENTE A LOS DELITOS INFORMÁTICOS

Fecha de presentación: 12 de marzo de 2002

Congresistas proponentes: José Barba Caballero y Hildebrando Tapia Samaniego

10.5.1. Fórmula legal

Artículo 1.- Modificase los artículos 207-A, 207-B y 207-C del Código Penal, promulgado por el Decreto Legislativo N.° 635, referente a Delitos Informáticos en los términos siguientes;

Capítulo X. Delitos Informáticos

Artículo 207-A.- El que utiliza o ingresa indebidamente a una base de datos, sistema o red de computadoras o cualquier parte de la misma, para diseñar, ejecutar o alterar un esquema u otro similar, o para interferir, interceptar, acceder o copiar información en tránsito o contenida en una base de datos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años o con prestación de servicios comunitarios de cincuentidós [sic] a ciento cuatro jornadas.

Si el agente actuó con el fin de obtener un beneficio económico, será reprimido con pena privativa de libertad no mayor de seis años o con prestación de servicios comunitarios no menor de ciento cuatro jornadas.

Artículo 207-B.- El que utiliza, ingresa o interfiere indebidamente una base de datos, sistema, red o programa de computadoras o cualquier parte de la misma con el fin de alterarlos, dañarlos o destruirlos, será reprimido con pena privativa de libertad no menor de cuatro ni mayor de seis años y con setenta a noventa días multa.

Artículo 207-C.- En los casos de los artículos 207-A y 207-B, la pena será privativa de libertad no menor de seis ni mayor de nueve años, cuando:

1. El agente accede a una base de datos, sistema o red de computadora, haciendo uso de información privilegiada, obtenida en función a su cargo.
2. El agente pone en peligro la seguridad nacional.

10.5.2. Considerando / Exposición de motivos

Véase el texto completo de esta exposición de motivos en el siguiente enlace:

10.5.3. Comentarios

En marzo de 2002, se presentó este proyecto de ley, el cual recoge la misma fórmula legislativa que la del proyecto 01744/2000-CR analizado anteriormente. Solo se diferencia el marco punitivo. Así, en el anterior proyecto se castigaba la primera modalidad base (art. 207-A) con no más de dos años de pena privativa de libertad; en este proyecto, la sanción oscila entre tres y seis años. La modalidad agravada (art. 207-A seg. párr.) se castigaba con no más de tres años, en el actual con no más de seis.

En el anterior proyecto se propuso que la segunda modalidad (art. 207-B) se castigue con una sanción de no menos de tres ni más de cinco años; en cambio, en la propuesta actual se considera una pena privativa de libertad no menor de cuatro ni mayor de seis años.

Finalmente, en el anterior proyecto se proponía que las circunstancias agravantes (art. 207-C) se castiguen con no menos de cinco ni más de siete años. El proyecto bajo análisis incrementó el castigo a una pena no menor de seis ni mayor de nueve años. Como se puede apreciar, para el legislador de inicios del siglo XXI, el endurecimiento de la represión era la respuesta adecuada al incremento de la ciberdelincuencia.

En la exposición de motivos se señala que algo atractivo de este tipo de delitos es la posibilidad de no ser descubiertos. De este modo, pese a que no

lo destacan expresamente, se resalta una de las características centrales de la ciberdelincuencia: el anonimato. Si bien cuando un usuario se conecta a una dirección IP, en teoría, es posible individualizarlo, puede suceder que el uso de direcciones IP dinámicas, redes abiertas (cibercafés, locutorios, wifi ajenas) o *softwares* libres especializados como la red TOR (The Onion Router) dificulten esta labor a las autoridades[893].

Adicionalmente, se precisa que quienes cometen estos actos delictivos tendrían *conocimientos especiales*. Como se ha dicho a lo largo de esta obra, esta es una generalización que, lejos de ayudar, genera sesgos en la investigación e, incluso, entre los ciudadanos que creen que todo acto ilícito cometido a través de las TIC lo realiza un *hacker*, cuando no es así.

Finalmente, la exposición de motivos resalta la necesidad de capacitación de nuestros operadores jurídicos: policías, fiscales y jueces. El lector debe recordar que la Divindat nace recién en el 2005, es decir, tres años después de la presentación de este proyecto de ley, mientras que las fiscalías especializadas en cibercrimen de Lima Centro se establecen casi 20 años después. Sin lugar a dudas, el legislador tenía mucha razón sobre la ausencia de preparación y necesidad de formación -la cual, lamentablemente, subsiste a la fecha-.

---

893 "El anonimato es una de las características particulares de esta moderna tecnología de la información y la comunicación. Las posibilidades de conocer con exactitud la identidad de los usuarios en las redes telemáticas son infinitamente menores en comparación con otros tipos de comunicación intersubjetivas. Existe un halo de misterio sobre la individualidad y personalidad de aquellos que acuden a esta forma de comunicación global, sumado a la falta de precauciones que generalmente se observa en la participación de los usuarios de Internet al suministrar datos personales o sensibles que pueden ser utilizados en su contra por terceros" (Aboso, *Derecho penal cibernético: La cibercriminalidad y el derecho penal en la moderna sociedad de la información y la tecnología de la comunicación*, cit., pp. 31 y s). En la misma línea: "El cibercrimen no tiene fronteras, porque Internet tampoco las tiene, la gran red de redes permite que desde una locación remota y escudado bajo el "anonimato" que le brinda estar detrás de un teclado, un individuo pueda cometer un delito en otra jurisdicción, en otro país o en otro continente. Es aquí donde los aspectos legales de la persecución de este tipo de delitos juegan un papel preponderante" (Sallis, Ezequiel. "Desafíos de la investigación de los delitos informáticos en la Deep & Dark Web". En: Dupuy, Daniela [dir.] y Mariana Kiefer [coord.]. *Cibercrimen. Aspectos de derecho penal y procesal penal. Cooperación internacional. Recolección de evidencia digital. Responsabilidad de los proveedores de servicios de Internet.* Montevideo: B de F, 2019, p. 603).

Los sólidos argumentos expuestos en este proyecto de ley cuentan con respaldo en la doctrina especializada de su época, cuyas reflexiones siguen siendo vigentes en la actualidad. Un ejemplo de ello se encuentra en un texto clásico del profesor Ulrich Sieber, publicado en 1992, donde se identifican cuatro características fundamentales de esta tipología delictiva: (1) permanencia y automatismo del hecho, (2) acumulación de daños, (3) magnitud y evolución futura de la criminalidad informática y (4) dificultades en su investigación[894].

10.6. PROYECTO DE LEY N.º 7197/2003-CR, LEY QUE INCORPORA NUEVAS FIGURAS DELICTIVAS AL CÓDIGO PENAL SOBRE LOS DELITOS INFORMÁTICOS

Fecha de presentación: 13 de junio de 2003

Congresista proponente: Martha Hildebrandt Pérez Treviño

10.6.1. Fórmula legal

Ley que incorpora el artículo 207-D al Código Penal sobre los delitos informáticos

Artículo 1.- Objeto de la norma.

Incorpórese el artículo 207-D al Código Penal, el cual constará en los siguientes términos:

Artículo 207-D.- El agente que se sirve de páginas web de carácter privado, sin conocimiento de su titular, para crear vínculos con otras páginas web será reprimido con pena privativa de libertad no mayor de dos años o con prestaciones de servicios comunitarios de cincuenta y dos a ciento cuatro jornadas.

Si el agente actuó con el propósito de obtener un beneficio económico o con el de perpetrar otro delito, será reprimido con pena privativa de libertad no mayor de tres años o con prestación de servicios comunitarios no menor de ciento cuatro jornadas.

894 Sieber, Ulrich. "Criminalidad informática: Peligro y prevención". En: Mir Puig, Santiago (coord.). *Delincuencia informática*. Barcelona: PPU, 1992, pp. 29-33.

10.6.2. Exposición de motivos

Véase el texto completo de esta exposición de motivos en el siguiente enlace:

10.6.3. Comentarios

La exposición de motivos de este proyecto de ley inicia con una definición que se asimila a la descrita en esta obra y que permite identificar los *computer crimes*, pues se dice que los delitos informáticos son aquellos comportamientos criminales en los que "la computadora está involucrada como material, objeto o mero símbolo". Sin embargo, el tipo penal propuesto corresponde a lo que hemos descrito como cibercrimen, ya que se trata de evitar y castigar conductas cometidas en el ciberespacio.

De este modo, luego de señalar que en el 2000 se insertaron al Código Penal tres delitos informáticos, se propone sancionar una conducta conocida como *inserción de enlaces maliciosos* en sitios legítimos:

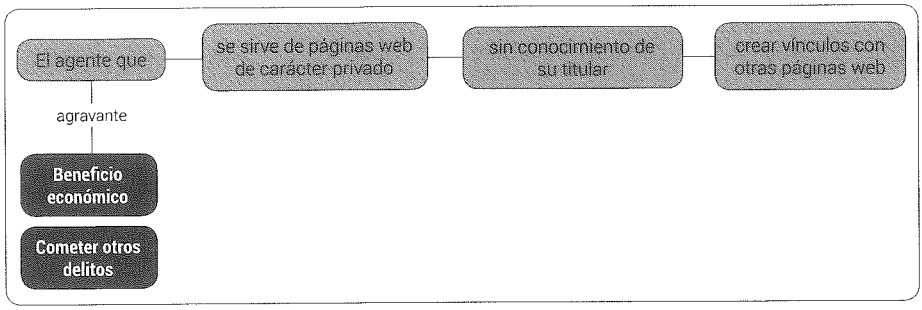


Diagrama 31. Estructura del delito de inserción de enlaces maliciosos en páginas legítimas, propuesto en el PL N.º 7197/2003-CR. Elaboración propia.

En la exposición de motivos se describen dos escenarios: (i) cuando el ilícito es cometido por alguien que tiene acceso de forma legítima -se menciona al diseñador o desarrollador de la web, pero podríamos generalizarlo al *insider*- y (ii) cuando el ilícito es cometido por el que quiebra las medidas de seguridad para realizar las modificaciones -agente externo-.

De otro lado, se proponen como agravantes dos escenarios:

a) Cuando se insertan para obtener un beneficio económico. Este supuesto ocurriría, por ejemplo, si el enlace conduce a un sitio web en el que se ofrecen productos o servicios prohibidos. También si se aprovecha la veracidad del sitio atacado para reconducir al visitante a uno suplantador en el que se ofrecen productos o servicios que no se entregarán.

b) Cuando se insertan para cometer otros delitos. En este caso, la página oficial reconduce a otra página cuya finalidad no es la obtención de rédito económico. Por ejemplo, la distribución de material de abuso sexual infantil o de *malware* destructivo.

Este proyecto no fue aprobado y esta modalidad no fue recogida. No es necesaria, ya que, de manera mucho más amplia, este tipo de conductas se podría calificar como ataque a la integridad de datos informáticos.

10.7. PROYECTO DE LEY N.° 10079/2003-CR, LEY QUE MODIFICA EL ART. 207-B Y AGREGA AL CAPÍTULO X (DELITOS INFORMÁTICOS) DEL TÍTULO V DEL CÓDIGO PENAL, LOS ARTS. 207-D, 207-E, 207-F Y 207-G

Fecha de presentación: 17 de marzo de 2004

Congresista proponente: Pedro Morales Mansilla

10.7.1. Fórmula legal

Ley que modifica el art. 207-B y agrega al Capítulo X Delitos Informáticos del Título V del Código Penal los artículos 207-D, 207-E, 207-F y 207-G.

Artículo 1.- Modificase el artículo 207-B del Código Penal, el mismo que quedará redactado con el siguiente texto:

Artículo 207-B.- Son responsables de fraude informático, las personas que valiéndose de cualquier método o modo, alteren, interfieran, manipulen, modifiquen o utilicen el funcionamiento de un programa informático, sistema informático, red, telemático o un mensaje de datos para procurarse la transferencia no consentida de los bienes, valores, derechos o patrimonio de otra persona en perjuicio de ésta o de un

tercero, serán sancionados con pena privativa de libertad no menor de tres años ni mayor de cinco años y con noventa a ciento veinte días multa.

Artículo 2.- Agregase al Capítulo X Delitos Informáticos del Título V del Código Penal los artículos 207-D, 207-E, 207-F y 207-G, los mismos que quedarán redactados con los siguientes textos:

Artículo 207-D.- Son responsables del delito de daños informáticos, la persona o personas que de cualquier modo o utilizando cualquier método destruyan, alteren, inutilicen, supriman o dañen los programas, datos, base de datos, información o cualquier mensaje de datos contenidos en un soporte lógico, sistema de información o telemático, y serán reprimidas con pena privativa de libertad no menor de tres ni mayor de cinco años y con sesenta a ciento ochenta días multa.

Serán reprimidos con la pena privativa de libertad no menor de cinco ni mayor de siete años y con sesenta a doscientos días multa, los que además destruyan o inutilicen la infraestructura e instalaciones físicas necesarias para la transmisión, recepción o codificación de los mensajes de datos.

(...)

Artículo 207-F.- Son responsables de intrusión indebida a los sistemas informáticos, de información o telemáticos la persona o personas que por cualquier medio o fin, y con el ánimo de apoderarse de la información contenida en dichos sistemas, o para descubrir los secretos comerciales o industriales, o bien para vulnerar la intimidad de una persona natural o jurídica, o simplemente vulnerar su seguridad, sin su consentimiento o autorización, interfieran, interrumpan, accedan a sistemas de información, conozcan o se apoderen de cualquier mensaje de datos. Serán reprimidas con pena privativa de libertad no menor de uno ni mayor de tres años y con sesenta a ciento veinte días multa.

La divulgación o la utilización fraudulenta de información reservada, los secretos comerciales o industriales que han sido obtenidos por alguna de las formas indicadas en el párrafo anterior será sancionada con pena privativa de libertad no menor de cuatro ni mayor de siete años y con noventa a trescientos días multa.

Si la divulgación o la utilización fraudulenta de los datos o información reservada, los secretos comerciales o industriales, se realiza por la persona o personas a las cuales se les encomendó su custodia o utiliza-

ción, serán sancionadas con una pena privativa de libertad no menor de cinco ni mayor de ocho años, con cien a trescientos días multa e inhabilitación para desempeñar cargos iguales o similares.

La violación de la reserva al secreto profesional será sancionada de acuerdo a lo dispuesto en el artículo 165 del Código Penal.

(...)

10.7.2. Exposición de motivos

Véase el texto completo de esta exposición de motivos en el siguiente enlace:



10.7.3. Comentarios

Este proyecto de ley fue presentado en marzo de 2004, es decir, cuatro años después que los primeros delitos informáticos se incorporasen al Código Penal. El paso de tiempo demuestra una mayor y mejor comprensión del fenómeno delictivo estudiado -pese a que continúa identificando la comisión de este tipo de delitos a personas con ciertos conocimientos técnicos-.

Si bien al inicio de este capítulo indiqué que evitaría transcribir delitos informáticos que no afecten la seguridad informática, en este proyecto de ley hago la excepción e incluyo el artículo 207-A CP, en tanto recoge una modalidad de fraude informático que incorpora diferentes tipos de manipulaciones a los sistemas informáticos.

Sobre la actividad delictiva contra la seguridad informática, este proyecto de ley propone dos ilícitos: (1) daños informáticos e (2) intrusismo indebido a los sistemas informáticos. En este sentido, en la exposición de motivos se indica que el bien jurídico protegido es la *información*, toda vez que el comercio y las relaciones sociales descansan en una adecuada administración de los entornos digitales, por lo que el Estado debe garantizar tanto la seguridad como la privacidad.

Si bien se resalta la naturaleza de estos delitos, así como sus características e importancia, se sigue asumiendo que estos delitos son cometidos por especia-

listas, cuando no es así necesariamente. De este modo, se utilizan expresiones como: "Se trata de una delincuencia de especialistas capaces muchas veces de borrar toda huella de los hechos" y "son conductas criminales de cuello blanco (*white collar crime*), en tanto que solo un determinado número de personas con ciertos conocimientos (en este caso técnicos) pueden llegar a cometerlas". En esta obra se han plasmado los argumentos que refuerzan nuestra posición: no se requiere contar con conocimiento técnico alguno, aunque haya especialistas que los tengan y delincan.

El delito de daños informáticos propuesto en este proyecto de ley recogería la siguiente estructura:

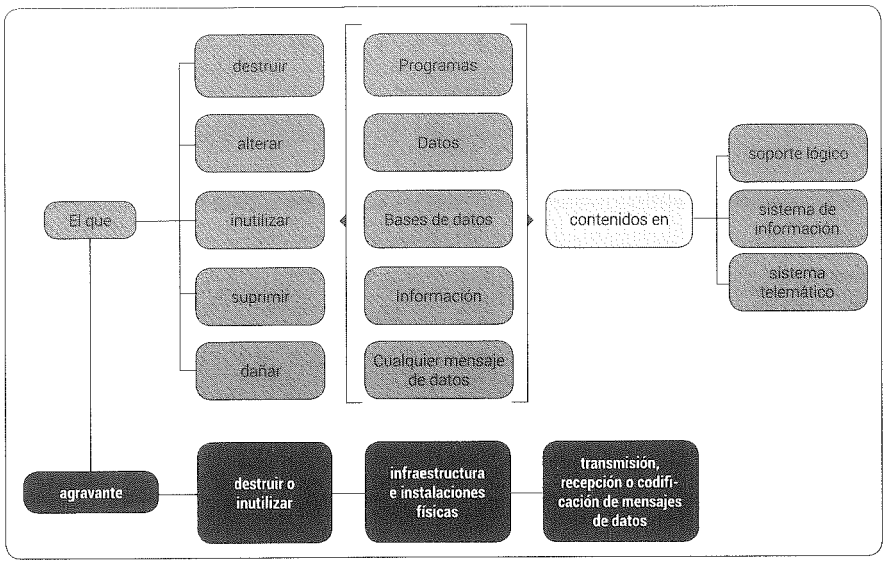


Diagrama 32. Estructura del delito de daños informáticos, propuesto en el PL N.º 10079/2003-CR. Elaboración propia.

El delito de acceso ilícito y divulgación de información obtenida, propuesto en este proyecto, recogería la siguiente estructura:

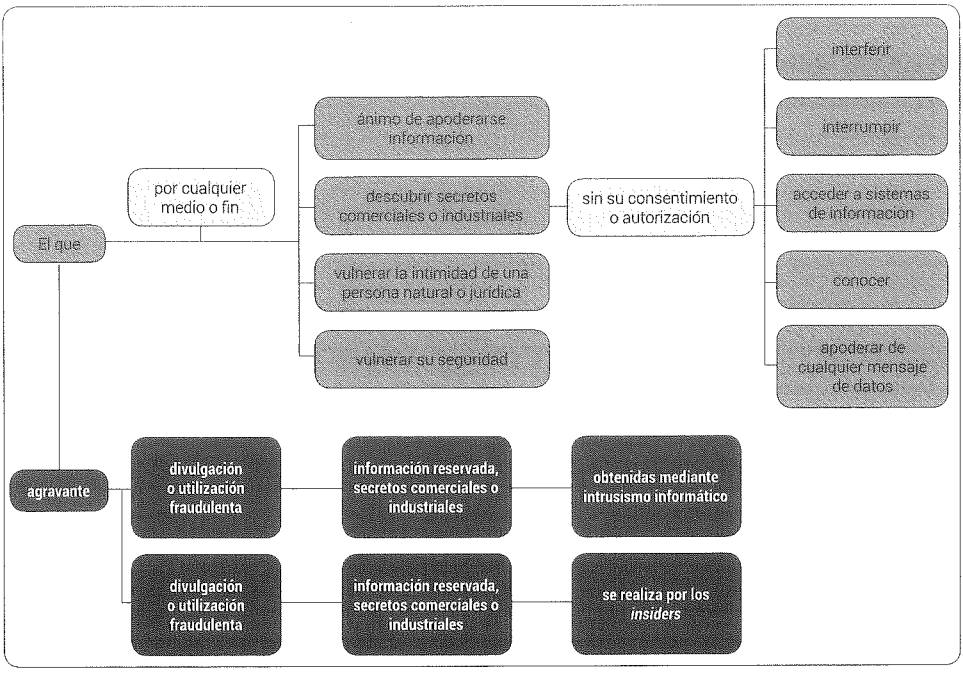


Diagrama 33. Estructura del delito de intrusismo indebido a los sistemas informáticos, propuesto en el PL N.° 10079/2003-CR. Elaboración propia.

Como se puede apreciar, el segundo delito incluye como modalidad agravada una conducta ajena al intrusismo informático: la divulgación o utilización de información previamente obtenida de los sistemas informáticos. Esta técnica legislativa no es adecuada, ya que, de un lado, no sigue las recomendaciones previstas en el Convenio de Budapest y, de otro, incluye una conducta autónoma o independiente que no necesariamente está relacionada con el acceso indebido.

Finalmente, el segundo delito propuesto precisa innecesariamente que la violación del secreto profesional será sancionada de conformidad con el artículo 165 CP.

10.8. PROYECTO DE LEY N.° 11346/2004-CR, LEY QUE INCORPORA NUEVAS FIGURAS DELICTIVAS AL CÓDIGO DE JUSTICIA MILITAR

Fecha de presentación: 06 de setiembre de 2004

Congresista proponente: Pedro Morales Mansilla

10.8.1. Fórmula legal

Proyecto de Ley que incorpora nuevas figuras delictivas al Código de Justicia Militar

Artículo 1.- Incorpórese los delitos informáticos al Decreto Ley N.º 23214, Código de Justicia Militar, el que queda redactado de la siguiente manera:

Artículo.- El militar que ingresa indebidamente a una base de datos, sistema o red de computadoras o cualquier parte de la misma, para interferir, interceptar, acceder o copiar información en tránsito o contenida en una base de datos será reprimido con reclusión militar no menor de un año.-

Artículo.- La divulgación o la utilización fraudulenta de los datos o información reservada y de los secretos militares, realizada por militares a quienes se les encomendó su custodia o utilización, será reprimida con pena privativa de libertad no menor de cinco ni mayor de doce años e inhabilitación para desempeñar cargos similares.

Artículo.- Es responsable de intrusión indebida a los sistemas informáticos, de información o telemáticos, el militar que por cualquier medio o fin, y con el ánimo de apoderarse de la información contenida en dichos sistemas, o para descubrir los secretos militares, o para vulnerar la seguridad militar sin consentimiento o autorización interfiera, interrumpa, acceda a sistema de información, conozca o se apodere de cualquier mensaje de datos, será reprimido con pena privativa de libertad ni menor de dos ni mayor de cinco años.

La divulgación de los secretos militares que han sido obtenidos por algunas de las formas indicadas en el párrafo anterior será sancionada con pena privativa de libertad no menor de cuatro ni mayor de diez años.

Artículo.- Circunstancias agravantes.

En el caso de los artículos anteriores la pena será privativa de libertad no menor de ocho ni mayor de quince años, cuando el militar pone en peligro la seguridad nacional.

10.8.2. Exposición de motivos

Véase el texto completo de esta exposición de motivos en el siguiente enlace:	

10.8.3. Comentarios

En este proyecto de ley se recomienda incorporar los delitos informáticos al Código de Justicia Militar, específicamente el acceso ilícito y la divulgación de información ilegalmente obtenida. Sin embargo, como se anotará en líneas posteriores, la técnica legislativa es inadecuada, pues regula modalidades de acceso ilícito en dos artículos diferentes.

El delito de ingreso indebido propuesto incluye un elemento subjetivo trascendente, pues no se sanciona únicamente al militar que accede a un sistema informático (mero intrusismo), sino al que lo hace con una finalidad ilegal: interferir, interceptar, acceder o copiar información en tránsito o contenida en bases de datos.

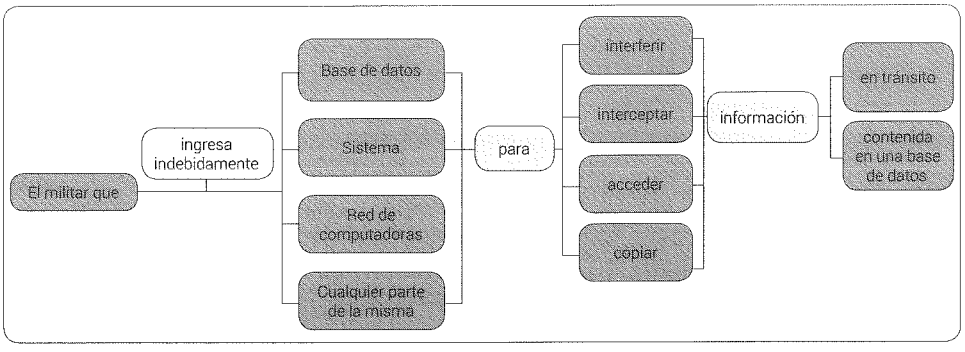


Diagrama 34. Estructura del delito de ingreso indebido, propuesto en el PL N.º 11346/2004-CR. Elaboración propia.

El segundo delito propuesto sanciona al militar que previamente recibió en custodia o bajo encomendación datos informáticos, información reservada o secretos militares, pero que indebidamente los divulga o utiliza para fines distintos.

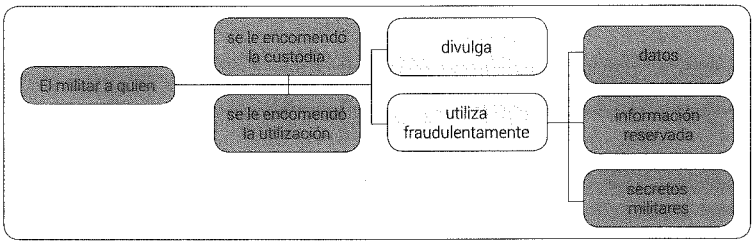


Diagrama 35. Estructura del delito de divulgación o utilización fraudulenta de datos, propuesto en el PL N.º 11346/2004-CR. Elaboración propia.

Este tercer delito es denominado como *intrusión indebida* en el proyecto de ley, sin embargo, su estructura se asemeja al de interceptación de datos informáticos. Pese a ello, se advierte que el legislador consideraba relevante incluir una finalidad adicional, esto es, no limitarse a sancionar las conductas dolosas, sino que debería acreditarse que el agente actuó con un ánimo adicional: apoderarse de información, descubrir secretos o vulnerar la seguridad militar.

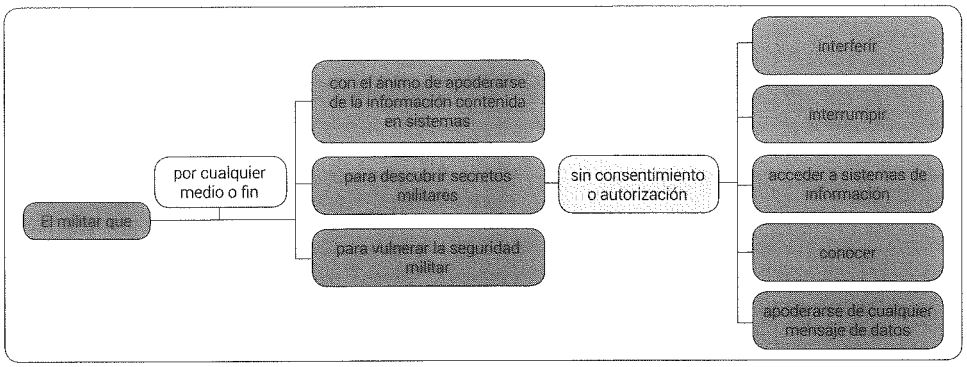


Diagrama 36. Estructura del delito de intrusión indebida, propuesto en el PL N.º 11346/2004-CR. Elaboración propia.

Al margen de los cuestionamientos sobre la técnica legislativa empleada, es importante reconocer el esfuerzo del legislador peruano para identificar los espacios que aún no recogían los delitos informáticos, pero que devenían en necesarios. En este caso particular, el fuero militar.

10.9. PROYECTO DE LEY N.º 11402/2004-CR, LEY QUE MODIFICA EL ART. 207-A DEL CÓDIGO PENAL REFERIDO A LOS DELITOS INFORMÁTICOS

Fecha de presentación: 10 de setiembre de 2004

Congresista proponente: Juan de Dios Ramírez Canchari

10.9.1. Fórmula legal

Ley que modifica el artículo 207-A del Código Penal respecto a los delitos informáticos

Artículo 1.- Objeto de la ley.

Modificase el artículo 207-A previsto en el Capítulo X Título V Libro Segundo del Código Penal, en los siguientes términos:

> Artículo 207-A.- El que utiliza o ingresa indebidamente a una base de datos, sistema o red de computadoras o cualquier parte de la misma, para diseñar, ejecutar o alterar un esquema u otro similar o para interferir, interceptar, acceder a copiar información en tránsito o contenida en una base de datos, será reprimido con pena privativa de libertad no mayor de cuatro años o con prestación de servicios comunitarios de 52 a 104 jornadas.
>
> Si el agente actuó con el fin de obtener un beneficio económico será reprimido con pena privativa de libertad no mayor de 06 años o con prestación de servicios comunitarios no menor de ciento cuatro jornadas.

10.9.2. Exposición de motivos

Véase el texto completo de esta exposición de motivos en el siguiente enlace:



10.9.3. Comentarios

A través de la propuesta analizada, se sugirió elevar la pena del denominado *delito informático*, previsto en el artículo 207-A CP al considerar que la sanción no era acorde a la magnitud del daño ni el impacto social producido. De este modo, el *acceso ilícito* -recogido en el primer párrafo- elevaría el castigo de dos a cuatro años de pena privativa de libertad. De otro lado, si el agente perseguía una finalidad económica -modalidad agravada prevista en el segundo párrafo-, el castigo máximo pasaría de tres a seis años.

Considero que este proyecto de ley descansa en fundamentos correctos: la delincuencia informática o la ciberdelincuencia es un fenómeno delictivo que debe ser sancionado con penas proporcionales a la lesión del bien jurídico y, hoy en día, la *seguridad informática* es uno sumamente valioso. Asimismo, en este proyecto se hace bien al comparar la sanción que recibe el delito de estafa con aquella modalidad informática que origina un beneficio económico indebido, ya que los delitos tradicionales nos proporcionan un buen punto de comparación en lo que al marco punitivo se refiere.

Sancionar este tipo de conductas con penas mínimas de dos años afectan la eficacia de la investigación criminal, ya que el Ministerio Público tendría

que obtener información de los proveedores de servicios de internet de manera inmediata, individualizar al agente, acusarlo, llevarlo a juicio oral y obtener una sentencia firme en muy poco tiempo; caso contrario, la *prescripción extraordinaria* del delito favorecería al ciberdelincuente.

10.10. PROYECTO DE LEY N.° 1318/2006-CR, LEY DE REPRESIÓN DE LOS DELITOS INFORMÁTICOS

Fecha de presentación: 21 de mayo de 2007

Congresista proponente: Célula Parlamentaria Aprista

10.10.1. Fórmula legal

Ley de represión de los delitos informáticos

Capítulo I. Objeto de la ley

Artículo 1.- Objeto. La presente ley tiene por objeto proteger y privilegiar la buena fe y la confiabilidad puesta en la informática como un instrumento que favorece el desarrollo humano y que contribuye a mejorar la vida de la población en su conjunto, frente a toda aquella conducta antisocial que amenace o atente contra estos valores.

Capítulo II. Delitos contra los sistemas que utilizan tecnologías de información

Artículo 2.- Acceso indebido. El que sin la debida autorización o excediendo la que hubiere obtenido, acceda, intercepte, interfiera o use un sistema que utilice tecnologías de información, será reprimido con pena privativa de libertad no menor de uno ni mayor de tres años.

Artículo 3.- Sabotaje o daño a sistemas. El que destruya, dañe, modifique o realice cualquier acto que altere el funcionamiento o inutilice un sistema que utilice tecnologías de información o cualquier de los componentes que lo conforman, será reprimido con pena privativa de la libertad no menor de uno ni mayor de seis años.

Incurrirá en la misma pena quien destruya, dañe, modifique o inutilice la data o la información contenida en cualquier sistema que utilice tecnologías de información o en cualquiera de sus componentes.

La pena privativa de libertad será no menor de tres años, si los efectos indicados en el presente artículo se realizaren mediante la creación, introducción o transmisión, por cualquier medio, de un virus informático o programa análogo.

Artículo 4. Acceso indebido o sabotaje a sistemas protegidos. Las penas previstas en los artículos anteriores se aumentarán entre una tercera parte y la mitad cuando los hechos allí previstos o sus efectos recaigan sobre cualquiera de los componentes de un sistema que utilice tecnologías de información protegido por medidas de seguridad, que esté destinado a funciones públicas o que contenga información personal o patrimonial de uso restringido sobre personas o grupos de personas naturales o jurídicas.

Artículo 5. Posesión de equipos o prestación de servicios de sabotaje. El que, con el propósito de destinarlos a vulnerar o eliminar la seguridad de cualquier sistema que utilice tecnologías de información, importe, fabrique, posea, distribuya, venda o utilice equipos o dispositivos; o el que ofrezca o preste servicios destinados a cumplir los mismos fines, será reprimido con pena privativa de libertad no menor de uno ni mayor de tres años.

Artículo 6. Espionaje informático. El que indebidamente obtenga, revele o difunda la data o información contenidas en un sistema que utilice tecnologías de información o en cualquiera de sus componentes, será reprimido con pena privativa de la libertad no menor de uno ni mayor de seis años.

La pena se aumentará de un tercio a la mitad, si el delito previsto en el presente artículo se cometiere con el fin de obtener algún tipo de beneficio para sí o para otro.

El aumento será de la mitad al doble, si se pusiere en peligro la seguridad del Estado, la confiabilidad de la operación de las instituciones afectadas o resultare algún daño para las personas naturales o jurídicas como consecuencia de la revelación de las informaciones de carácter reservado.

(...)

Capítulo IV. Delitos informáticos contra la privacidad de las personas y de las comunicaciones

Artículo 15.- Violación de la privacidad de la data o información de carácter personal. El que por cualquier medio se apodere, utilice, modifique o elimine, sin el consentimiento de su dueño, la data o in-

formación personales de otro o sobre las cuales tenga interés legítimo, que estén incorporadas en un computador o sistema que utilice tecnologías de información, será reprimido con pena privativa de libertad no menor de uno ni mayor de tres años.

La pena se incrementará de un tercio a la mitad si como consecuencia de los hechos anteriores resultare un perjuicio para el titular de la data o información o para un tercero.

Artículo 16.- Violación de la privacidad de las comunicaciones. El que, mediante el uso de tecnologías de información, accede, capture, intercepte, interfiera, reproduzca, modifique, desvíe o elimine cualquier mensaje de datos o señal de transmisión o comunicación ajenos, será reprimido con pena privativa de libertad no menor de dos ni mayor de cinco años.

Artículo 17.- Revelación indebida de data o información de carácter personal. El que revele, difunda o ceda, en todo o en parte, los hechos descubiertos, las imágenes, el audio o, en general, la data o información obtenidos por alguno de los medios indicados en los artículos precedentes, aun cuando el autor no hubiese tomado parte en la comisión de dichos delitos, será reprimido con pena privativa de libertad no menor de uno ni mayor de tres años.

Si la revelación, difusión o cesión se hubieren realizado con un fin de lucro o si resultare algún perjuicio para otro, la pena aumentará de un tercio a la mitad.

(...)

10.10.2. Exposición de motivos

Véase el texto completo de esta exposición de motivos en el siguiente enlace:	

10.10.3. Comentarios

Este proyecto de ley destaca la importancia de la informática en la vida de los seres humanos, así como su impacto en el plano laboral, social, profesional y político. Además, pese a haberse presentado en mayo del 2007, menciona expresamente *la investigación en el campo de la inteligencia artificial.* Así, si bien

en el 2025 discutimos sobre su regulación y las implicancias en el derecho penal, hace casi dos décadas, un grupo de legisladores ya avizoraban estos escenarios.

De otro lado, se resalta que, si bien Estados Unidos, Europa Occidental, Australia y Japón han sido los países más afectados por ciberataques, a nivel mundial, nuestro país no puede permanecer ajeno a este escenario dado que el volumen de información se erige como el nuevo norte de la delincuencia por la facilidad con la que se pueden ocultar las huellas y proteger el anonimato, así como las ganancias que se pueden obtener al atacar sistemas informáticos de empresas o entidades financieras.

Al igual que otros proyectos de ley previamente comentados, en este también se cita el trabajo del tratadista mexicano Julio Téllez Valdéz al describir las características de la delincuencia informática. Sin embargo, en este proyecto se destaca la importancia de capacitar a nuestros operadores jurídicos para que puedan enfrentar un tipo de delincuencia tan sofisticada y técnica.

Este proyecto, de forma adecuada, identifica algunos tipos de ciberataques. Así, por ejemplo, como parte del sabotaje informático recoge tanto los atentados físicos como lógicos y, entre estos últimos, describe los más frecuentes en aquella época: Bombas lógicas y cáncer de rutinas -específicamente, el uso de virus-. Además, identifica tanto el acceso no autorizado a sistemas informáticos como el uso ilegítimo de estos y la divulgación de información confidencial.

La propuesta legislativa recoge un capítulo denominado «Delitos contra los sistemas que utilizan tecnologías de información». El primer delito que se propone sancionar es el acceso indebido. Aunque se castiga a quien no cuenta con autorización y a quien excede sus facultades, este delito no se limita al acceso indebido, sino también a la interceptación, interferencia o utilización de sistemas informáticos.

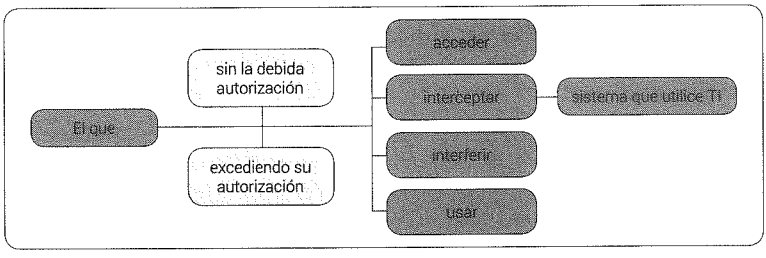


Diagrama 37. Estructura del delito de acceso indebido, propuesto en el PL N.º 1318/2006-CR. Elaboración propia.

En este proyecto también se recomienda sancionar los ataques contra la integridad y disponibilidad de los sistemas informáticos -bajo la denominación de *sabotaje o daños a sistemas-*. En el segundo párrafo se incluye también la data o información contenida en los sistemas en referencia, por lo que podemos afirmar que también recoge los *ataques contra la integridad y la disponibilidad de los datos informáticos*. Finalmente, en el último párrafo se precisa la sanción que debe recibir quien utiliza virus informáticos o programas análogos -entiéndase, *software* malicioso-.

La estructura del segundo delito propuesto sería la siguiente:

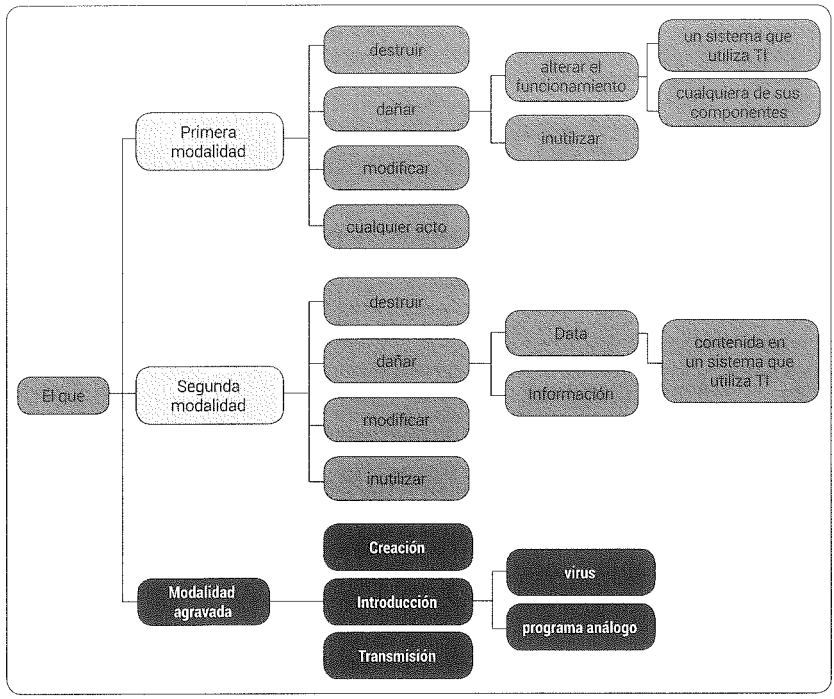


Diagrama 38. Estructura del delito de sabotaje o daños a sistemas, propuesto en el PL N.º 1318/2006-CR. Elaboración propia.

Es importante indicar que el proyecto de ley contempla como circunstancia agravante de los dos delitos analizados cuando los hechos o efectos recaigan sobre información o sistemas destinados a funciones públicas o que contengan información personal o patrimonial, sea de personas individuales, agrupaciones o personas jurídicas.

El tercer y último delito que comentar será el denominado *posesión de equipos o prestación de servicios de sabotaje*. Como señalé en el capítulo en donde desarrollamos el abuso de mecanismos y dispositivos informáticos, nuestro legislador emplea una inadecuada técnica legislativa al sancionar de forma independiente los actos de colaboración, pues puede hacerlo bajo las formas tradicionales de autoría y participación (complicidad, en este caso). Además, vemos que este proyecto de ley propone sancionar el mero ofrecimiento, lo que es una clara expansión del sistema punitivo -lo que se ha denominado como *hiperanticipación* y que también ha sido criticado en el capítulo en referencia-.

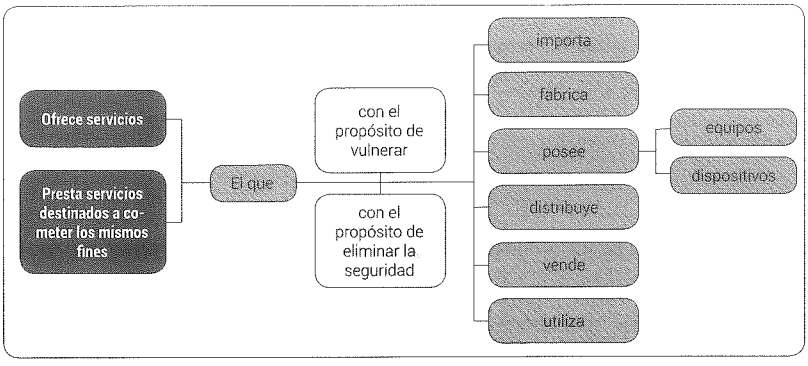


Diagrama 39. Estructura del delito de posesión de equipos o prestación de servicios de sabotaje, propuesto en el PL N.º 1318/2006-CR. Elaboración propia.

10.11. PROYECTO DE LEY N.º 1828/2007-CR, LEY QUE PENALIZA LOS DELITOS INFORMÁTICOS

Fecha de presentación: 31 de octubre de 2007

Congresista proponente: Álvaro Gutiérrez Cueva

10.11.1. Fórmula legal

Ley que penaliza los delitos informáticos

Capítulo I. Objeto de la ley

Artículo 1.- Objeto. La presente Ley tiene por objeto:

a) Proteger integralmente a los que utilicen tecnologías de información.

b) Prevenir la comisión de los delitos que se cometieran contra estos sistemas cualquiera de sus componentes, o los que fueran cometidos por medio de tecnologías, en los términos que a continuación se determinan.

Artículo 2.- Definición de términos. A los fines de la presente Ley, se detallan términos de informática cuyo significado se interpretará de acuerdo a las definiciones que se consignen:

1) Computadora: equipo que posee un conjunto de elementos electromecánicos y electrónicos con el propósito de procesar información, cumple funciones de control, borrado, recuperación, y de almacenamiento, entre otras. A ella se le incorpora cualquier instalación de almacenamiento de datos o de comunicaciones directamente relacionadas, u operativas en conjunción con dicho equipo.
2) BBS: o Sistema de Boletines Electrónicos, es un sistema de computación y asociación de software, que funciona como conmutación de mensajes, donde se centraliza la información para grupos de interés particular, que proveen de una base de datos donde los usuarios de computadoras pueden, enviar o recibir mensajes electrónicos.
3) Datos: Es la información que debe suministrarse a una computadora, preparados en forma adecuada para ser usados en sistemas de computación.
4) Programa de computación: hacen que la computadora o sistema de computación cumpla su función, mediante datos que se le incorporan y que representan instrucciones, declaraciones, etc.
5) Buffer: Es un dispositivo, usado para almacenar datos temporalmente.
6) CD-Rom: Es un disco compacto que se utiliza para almacenar y reproducir textos, videos, gráficos, sonidos y programas.
7) Ciperespacio: Es el espacio virtual donde una persona se encuentra cuando ha establecido una conexión y existe una comunicación en línea.
8) Cracker: es un individuo que trata de ingresar a sistemas y/o redes de computadoras mediante la violación de claves secretas de accesos con la intención de explorar dichos sistemas y redes, y reproducir y sacar provecho económico mediante la venta de eses sistema vulnerado

9) Cybertots: son las faltas menores o contravenciones cometidas al usar las computadoras.
10) Disco rígido: Es un tipo de soporte magnético, elemento del hardware de la computadora, que se usa para almacenar información.
11) Diskette: Es el soporte magnético portátil, utilizado para almacenar información, que se inserta en un dispositivo especifico de la computadora, para leer dicha información.
12) Encripción: Sistema de seguridad que realiza conversiones de información a cifrados, para evitar que terceros tengan acceso a ella
13) E-mail: Medio que permite enviar y recibir información desde una computadora o terminal, a una o más terminales, ubicadas en cualquier parte del mundo, siempre que se encuentren conectadas a través de redes de computadoras.
14) Firewall: Dispositivo con medidas especiales de seguridad de acceso, utilizado para servicios de conexiones externos, y para líneas de acceso de discado utilizado para proteger a las redes corporativas frente a solicitudes de ingreso no autorizadas, con el fin de controlar la información entrante y saliente de una red de computadoras.
15) Hacker: Es el individuo que con la finalidad de causar un daño, o bien obtener ilegalmente información de uso reservado, procura ingresar a las computadoras ajenas, para violar e investigar sus recursos de control.
16) Hardlock: es un dispositivo que si se conecta a una computadora, permite la ejecución de un programa, siendo usualmente su función, proteger el copiado de dicho programa.
17) Softlocks: es un programa de seguridad de software, también dar seguridad contra el copiado.
18) Internet: Internet es el conjunto total de redes interconectadas por medio de routers, entendiéndose como, la conexión a la red de todas las redes de computadoras, a nivel mundial.
19) Módem: Es el Dispositivo mediante el cual se convierten señales de datos analógicas en señales digitales y binarias, o viceversa, para hacer posible la utilización del medio por el cual se quiere recibir o transmitir información.
20) Multimedia: Sistema de facilidades para el manejo e intercambio de textos, gráficos, voz y vídeo en las computadoras.

21) Navegación: por medio de ella y con los programas diseñados para ese fin, se recorren los distintos servicios que ofrece una red.

22) Obras de informática: son las Obras de Base de Datos y las de Software.

23) Obras de base de datos: son las de categoría literarias, conjunto organizado de datos interrelacionados entre sí, recopilados para su procesamiento y recuperación, mediante técnicas y sistemas informáticos.

24) Obras de Software: son producciones constituidas por ej. para escuchar o grabar una función de un sistema de computación, o adquirir la sustancia, significado o propósito del mismo.

25) Servicios de información en línea: son servicios que ofrecen al público una capacidad para adquirir, procesar, guardar, generar, transformar, recuperar, utilizar, o hacer posible el acceso a una información, a través de telecomunicaciones, incluyendo servicios que permitan al cliente recuperar información almacenada, o información de archivos para almacenar en instalaciones de almacenamiento de datos; publicaciones electrónicas, y servicios de mensajería electrónica.

26) Enlace: Medio de telecomunicaciones de características específicas entre dos puntos.

27) Encriptado: Cualquier procedimiento usado en criptografía para convertir información en forma de texto, dato, imágenes o video, en signos ininteligibles para quien no disponga de la clave secreta para desencriptarlos a fin de prevenir cualquier intento de lectura de los mismos.

28) Hardware: Equipo de computadora físico qué soporta aplicaciones programas, posee todos los componentes que integran una computadora.

29) Host: Es la computadora de mayor jerarquía en una red informática interconectada.

30) Mailbox: Es una casilla de correo electrónico.

31) Multiplexor: Es el equipo que por medio de técnicas definidas, combina varios canales afluentes, en un número reducido de canales portadores combinados con una relación fija entre los mismos.

32) Nodo: Punto donde convergen dos líneas. Dispositivo físico que puede direccionarse mediante otro dispositivo.

33) Paquete de datos: es la unidad en que se divide la información a los efectos de transmitirla.

34) Password: es la información confidencial, que puede ser usada para la autenticación de un usuario, entidad o recurso.

35) Piratería informática: es el delito que consiste en la copia, distribución o locación de una obra de informática, sin la autorización de su propietario, para ser utilizada en forma personal, o bien para su venta, distribución, edición, almacenaje, importación o también, con el fin de facilitar otras conductas ilegales.

36) Programas: Son los diseños, tanto generales como detallados de los datos en un sistema de computación.

37) Red: Es el sistema de comunicaciones en el que las computadoras transfieren y comparten datos y recursos.

38) Router: es el dispositivo electrónico por el cual se encamina el tráfico de datos entre redes de trabajo.

39) Scanner: es dispositivo electrónico por medio del cual se pueden copiar imágenes y digitalizarlas.

40) Server: Una computadora que otorga algún tipo de servicio a otras computadoras que están conectadas, o a dos computadoras, a través de una red.

41) Sistemas: Son el conjunto de partes que realizar la misma función; o es el conjunto de objetos unidos por alguna forma de acción o interdependencia; o un complejo de entidades relacionadas entre sí.

42) Sistema operativo: es el soporte que controla la gestión y la ejecución de programas en una computadora o conjunto de ellas.

43) Sitio: lugar físico donde se encuentran los recursos informáticos, o se alojan programas o aplicaciones en Internet.

44) Soporte lógico: Programas de computadoras, procedimientos, reglas y toda la documentación asociada, para explotar un sistema de computación.

45) Soporte magnético: Es el medio de almacenamiento de información que admite el registro permanente de datos, y permite su lectura, escritura y borrado.

46) Telemática: Servicios de telecomunicación que completan los servicios telegráficos o telefónicos tradicionales, utilizando generalmente técnicas de teletratamiento para permitir que el usuario reciba o envíe información pública o privada, efectúe operaciones tales como la consulta de archivos, reservas o transacciones comerciales o bancarias.

47) Transferencia electrónica de fondos: Es la operatoria por medio de la cual un emisor, imparte una orden a un receptor, para que se acrediten o debiten fondos en una determinada cuenta.

48) Versión fuente: son los programas escritos en un pseudo lenguaje capaces de ser interpretados o leídos por una persona.

49) Versión objeto: son los programas capaces de ser interpretados por la computadora.

50) Virus: Es todo segmento de un programa que puede copiarse, para infectar a otros programas, a los que ataca modificándolos, destruyéndolos, etc. o con el fin de impedir el correcto funcionamiento de una computadora, red, o sistema.

Capítulo II: De los delitos contra la propiedad

Artículo 3.- Sanciones al delito

Será reprimido con pena de multa y sancionado correspondiente, si no resultare un delito más severamente penado, el que accediere, por cualquier medio, a una computadora, sistema de computación, medios de almacenamientos de datos, o a datos de computación, que no le pertenezcan sin que lo haya autorizado el propietario, o habiendo excedido los límites de la autorización que le hubieran conferido.

Exceptuase de lo dispuestos en el caso en que la computadora o sistema de computación, medios de almacenamiento de datos, o datos de computación, esté librados al acceso público, sin restricciones de ningún tipo; o que el acceso del autor no se encuentre comprendido entre las restricciones establecidas.

Artículo 4.- Multas al delito

La pena de multa será de 10 UIT (unidad impositiva tributaria), si el autor del hecho copia, ya sea para él o para otras personas, todo o parte de los datos a los que haya accedido.

En todo caso, si las conductas se dirigen a sistemas de datos informáticos concernientes a la seguridad, defensa nacional, salud pública o prestación de servicios públicos.

Capítulo III: Daño a datos informáticos

Artículo 5.- Manipulación del sistema de datos informáticos.

Será reprimido con prisión de seis meses a tres años, si el hecho no constituyera delito más severamente penado, quien sin expresa autorización del propietario, o excediendo los límites de la autorización que le fuera conferida, de cualquier modo y por cualquier modo destruyere, alterare, hiciere inutilizable o inaccesible, un sistema o datos informáticos.

Artículo 6.- Penas para quienes cometen los delitos contra la propiedad.

En los supuestos contemplados en el artículo tercero será reprimido con prisión de dos a ocho años, si mediare cualquiera de las siguientes circunstancias:

1. Si fuera cometida contra un sistema o datos pertenecientes a organismos de seguridad, defensa nacional o inteligencia, salud pública o la prestación de un servicio público.
2. Si fuera cometido contra un sistema o dato de valor científico o financiero.
3. Si el autor de la conducta punible se tratara del personal de la empresa u organismo público o privado que tenga a su cargo de manera directa o indirecta, el mantenimiento, seguridad u operación del sistema o datos informáticos.

Artículo 7.- Daños a la integridad física y salud de las personas

Si como consecuencia del hecho fuera puesta en peligro la prestación de servicios públicos, o la integridad física y salud de personas, la pena será de cinco a diez años de reclusión o prisión.

(...)

Capítulo V: Entrega, venta y distribución de medios destinados a cometer delitos previstos en este artículo

Artículo 10.- Comercialización de material para delinquir

Será reprimido con prisión de tres meses a tres años, el que haga entrega, distribuya, vendiera otros o publicitara equipos de cualquier índole o programas de computación, para facilitar la comisión de los delitos previstos en la presente ley.

La misma pena se aplicará a quien, con intención de cometer delitos, use, venda, tenga en control o custodia, o posea, equipos o programas aptos para obtener acceso no autorizado, a servicios de telecomunicaciones.

(...)

10.11.2. Exposición de motivos

Véase el texto completo de esta exposición de motivos en el siguiente enlace:

10.11.3. Comentarios

Este proyecto de ley representa un gran avance en lo que al entendimiento del fenómeno de la cibercriminalidad se refiere. Si bien en la exposición de motivos se incluyen algunas definiciones que equiparan al *hacker* con el ciberdelincuente -posición que en esta obra rechazamos-, lo cierto es que se aprecia la intención de comprender de forma íntegra el avance de la cibercriminalidad.

De este modo, el proyecto de ley incorpora un artículo inicial que recoge los objetivos de la propuesta normativa: proteger a los usuarios de las TIC y prevenir la comisión de los delitos cometidos por medio y contra la tecnología. Además, en un intento de aclarar los conceptos y las definiciones que se emplearán, presenta 50 términos informáticos. Podemos no estar de acuerdo con algunas definiciones, pero es un esfuerzo pedagógico que merece ser reconocido.

En la sistematización de los delitos, el legislador escoge una fórmula que combina posiciones tradicionales -como reconocer que el patrimonio es el bien jurídico protegido en el delito de acceso ilícito como modernas -al identificar

algunos delitos que afectan la seguridad informática, bajo el rótulo de daños informáticos-. A continuación, analizaremos algunos de los delitos propuestos.

El proyecto de ley recomienda sancionar el delito de acceso ilícito, siguiendo una fórmula similar a la argentina: *si no resultare un delito más severamente penado*, precisión innecesaria, pues en Perú este problema se soluciona siguiendo las reglas del concurso de delitos. Asimismo, precisa que si el sistema de información "esté librado al acceso público" o no existen restricciones establecidas, el hecho será atípico.

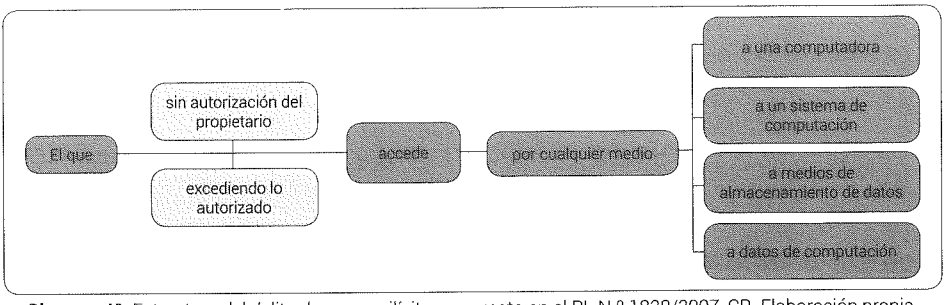


Diagrama 40. Estructura del delito de acceso ilícito, propuesto en el PL N.° 1828/2007-CR. Elaboración propia.

Este proyecto de ley también propone sancionar los ataques contra la integridad de los datos y sistemas informáticos, aunque bajo la denominación de *manipulación del sistema de datos informáticos*. Recordemos que, en esta época, la adhesión al Convenio de Budapest era lejana, razón por la cual se empleaban diferentes términos y fórmulas para proponer sanciones efectivas contra nuevas formas de criminalidad. En este caso, el objeto del delito serían tanto los sistemas informáticos como sus datos.

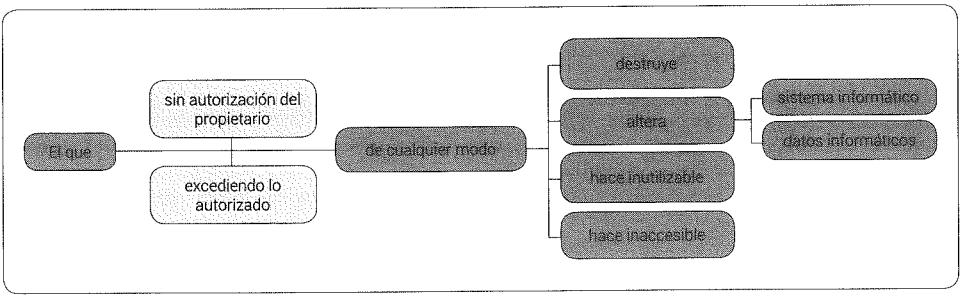


Diagrama 41. Estructura del delito de manipulación del sistema de datos informáticos, propuesto en el PL N.° 1828/2007-CR. Elaboración propia.

El último delito relevante en este análisis se denomina *comercialización de material para delinquir*, afín a nuestro actual delito de *abuso de mecanismos y dispositivos informáticos*, siendo la principal diferencia que, en la propuesta, se sugería sancionar, incluso, la posesión de los dispositivos. No obstante, tanto la propuesta legislativa como nuestra actual LDI no limitan los alcances de este ilícito, sino que los expanden a todo delito contemplado en la legislación especial -contra lo cual nos hemos pronunciado oportunamente-.

10.12. PROYECTO DE LEY N.° 3083/2008-CR, LEY QUE REGULA LOS DELITOS INFORMÁTICOS

Fecha de presentación: 12 de marzo de 2009

Congresistas proponentes: Juan Carlos Eguren Neuenschwander | Unidad Nacional

10.12.1. Fórmula legal

Este proyecto de ley se volvió a presentar en el siguiente periodo legislativo y fue la columna vertebral de la Ley de Delitos Informáticos.

10.12.2. Comentarios

Este proyecto de ley fue presentado el 12 de marzo de 2009, cuando el congresista Eguren Neuenschwander integraba el partido político Unidad Nacional. Pese a lo adelantado de su época, la propuesta no prosperó:

- El 13 de marzo de 2009 fue decretado a la Comisión de Justicia y Derechos Humanos del Congreso de la República.
- El 17 de marzo de 2009 fue recibido y se encontraba en la Comisión de Justicia y Derechos Humanos.
- El 23 de julio 2012 fue remitido al archivo, en 20 folios.

Es importante indicar que el congresista Eguren Neuenschwander persistiría, dos años después, con tan valiosa iniciativa legal. De este modo, el 11 de agosto de 2011, presentó el mismo proyecto de ley -esto es, la fórmula legislativa y la exposición de motivos-, pero con una nueva numeración y con Alianza por el Gran Cambio como nueva bancada. El Proyecto de Ley N.°

34/2011-CR será comentado más adelante, al ser uno de los ejes centrales en la evolución de la lucha contra la ciberdelincuencia.

Véase el texto completo de esta exposición de motivos en el siguiente enlace:

10.13. PROYECTO DE LEY N.º 4279/2010-CR, LEY QUE PROPONE CREAR UN SISTEMA REGULADOR Y SANCIONADOR RESPECTO AL USO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN (TICS)

Fecha de presentación: 02 de setiembre de 2010

Congresista proponente: Luis Humberto Falla Lamadrid

10.13.1. Fórmula legal

Ley especial de delitos informáticos que regula y sanciona a los usuarios infractores de la tecnología de información y comunicación

Título Único. Disposiciones

Artículo 1.- Por la presente Ley se definen nuevas figuras delictivas y se otorga facultades a la Policía Nacional para la obtención de información oportuna y la aplicación de herramientas legales para la lucha contra el crimen organizado y otros cometidos con tecnología que facilitan las actividades delictivas de las organizaciones criminales.

Artículo 2.- Agréguese al artículo 207-A Código Penal como delito informático, las siguientes figuras:

- El ingreso indebido para alterar, interferir, interceptar o copiar archivos magnéticos, electrónicos y/o digitalizados.
- Obtención indebida de claves de usuarios de uso virtual para la comunicación y/o transacciones financieras.
- La instalación de software o hardware espía en cualquiera de sus formas sin conocimiento del propietario o usuario del equipo.

Artículo 3.- También será considerado dentro del alcance del artículo 207-B, si para la ejecución del ilícito el agente emplea conocimiento técnico de intrusismo y/o cualquier tipo de software espía cuando son realizados a distancia.

(...)

Artículo 7.- Hacking Policial. La Policía Nacional del Perú tiene la facultad del empleo de la figura del Hacking Policial que consistirá en la utilización de las redes de computadoras, internet o las Tecnologías de la Información y Comunicaciones (TICs), para los siguientes casos:

- Evaluar o comprobar una acción o resultados compatibles con actividad criminal.
- Defender de un ingreso informático indebido inminente (intrusismo).
- Ubicar el medio utilizado e identificar a sus autores en los casos de delitos cometidos así como cuando se estén realizando transacciones relacionadas con otra actividad delictiva o cuando se realicen actos preparatorios para la comisión de un delito.

(...)

10.13.2. Exposición de motivos

Véase el texto completo de esta exposición de motivos en el siguiente enlace:

10.13.3. Comentarios

Este proyecto legislativo recomienda incluir nuevas modalidades delictivas como parte del artículo 207-A, *delito informático*, previsto en el CP. De este modo, sugiere sancionar: (1) el acceso ilícito que persigue una finalidad delictiva, es decir, no se propone sancionar el mero intrusismo, (2) la obtención de claves de usuarios que permitan la comunicación en línea o las transacciones financieras, (3) la instalación de *spyware* sin conocimiento o consentimiento del usuario titular del sistema.

De otro lado, el proyecto proponía ampliar los alcances del artículo 207-B CP para sancionar al agente que emplee conocimiento técnico especializado

relacionado al intrusismo informático y/o emplee cualquier tipo de *spyware* para realizar un ataque a distancia.

En este proyecto se sugiere habilitar el *hacking policial* para que los agentes puedan evaluar o comprobar acciones relacionadas a la actividad cibercriminal. De este modo, podrían tanto defender a los usuarios de un ataque indebido (acceso ilícito) como ubicar el medio técnico utilizado e individualizar a los ciberatacantes.

Finalmente, como dato curioso he de indicar que esta iniciativa legislativa incluye citas doctrinarias de autores que hemos identificado en proyectos previos: Julio Téllez Valdéz y Carlos Sarzana.

10.14. PROYECTO DE LEY N.º 34/2011-CR, LEY QUE REGULA LOS DELITOS INFORMÁTICOS

Fecha de presentación: 11 de agosto de 2011

Congresista proponente: Juan Carlos Eguren Neuenschwander

10.14.1. Fórmula legal

Ley de los delitos informáticos

Capítulo I

Generalidades

Artículo 1.- Objeto de la Ley

La presente ley tiene por objeto sancionar penalmente las conductas que afectan de manera relevante la confianza en la informática como instrumento que favorece el desarrollo humano y que contribuye a mejorar la calidad de vida de la población en su conjunto.

Artículo 2.- Glosario de Términos

Para los fines de la presente ley, entiéndase los siguientes conceptos de la siguiente manera:

a) Componentes de un sistema de información: comprende los diferentes elementos de hardware y software necesarios para el funcionamiento de sistemas y tecnologías de información.

b) Data o información: conjunto de datos contenidos en un sistema de información, integrados no volátiles y variables en el tiempo, que están orientados a un determinado ámbito (organización, empresa, etc.).

(...)

d) Sistema de información: conjunto de partes que funcionan relacionándose entre sí con el objetivo de capturar, almacenar y procesar información.

(...)

f) Tecnología de información: comprende los aspectos relacionados al hardware de un sistema de información, el cual comprende computadoras, servidores, equipos de comunicación y equipos de seguridad, así como los sistemas que permiten su operación y que son necesarios para el funcionamiento de los sistemas de información.

Capítulo II

Delitos contra los sistemas de información y las Tecnologías de Información

Artículo 3.- Intrusismo informático

El que sin la debida autorización acceda, intercepte o interfiera un sistema de información o una tecnología de información, será reprimido con una pena privativa de libertad no menor de uno ni mayor de tres años.

Artículo 4.- Sabotaje informático

El que destruya, dañe, modifique o realice cualquier acto que altere el normal funcionamiento o inutilice un sistema de información o una tecnología de información o cualquiera de los componentes que los conforman, será reprimido con pena privativa de la libertad no menor de uno ni mayor de seis años.

Se le impondrá la misma pena a quien destruya, dañe, modifique o inutilice la data o la información contenida en cualquier sistema de información o tecnología de información o en cualquiera de sus componentes.

La pena privativa de la libertad será no menor de tres ni mayor de seis, si la alteración o inutilización se llevase a cabo mediante la creación, introducción o transmisión, por cualquier medio, de un virus informático o programa análogo capaz de extenderse a otros sistemas de información sus componentes.

Artículo 5.- Intrusismo o sabotaje de sistemas o tecnologías de información con medidas de seguridad o con información especial

La pena será privativa de libertad no menor de cuatro ni mayor de siete años si los delitos previstos en los artículos precedentes recaen sobre cualquiera de los componentes de un sistema de información o de una tecnología de información protegidos por medidas de seguridad, que este destinado a funciones públicas o servicios privados que contenga información personal o patrimonial reservada sobre personas naturales o jurídicas.

Artículo 6.- Prestación de equipos y servicios con fines de intrusismo y/o sabotaje

El que importe, fabrique, posea, distribuya, venda o utilice equipos o dispositivos con el propósito de destinarlos a vulnerar o eliminar la seguridad de cualquier sistema de información o de una tecnología de información, o el que ofrezca o preste servicios que contribuyan a ese propósito, será reprimido con pena privativa de libertad no menor de uno ni mayor de tres años.

Artículo 7.- Espionaje informático

El que indebidamente obtenga, revele o difunda la data o información contenidas en un sistema de información o en una tecnología de información o en cualquiera de sus componentes, será reprimido con pena privativa de libertad no menor de uno ni mayor de seis años.

La pena privativa de la libertad será no menor de tres ni mayor de siete años si el delito se cometiere con el fin de obtener algún tipo de beneficio para sí o para otro.

La pena privativa de la libertad será no menor de cuatro ni mayor de diez si como consecuencia de dicho acto se pusiere en peligro la seguridad del Estado, la confiabilidad general de las operaciones financieras o administrativas de las instituciones públicas o privadas afectadas o resultare algún daño relevante para las personas naturales o jurídicas.

Capítulo III

Delitos informáticos contra la intimidad y el secreto de las comunicaciones

Artículo 8.- Violación de la intimidad de la data personal

El que por cualquier medio se apodere, utilice, modifique o elimine sin el consentimiento del titular la data o información personal de otro

que estén incorporadas en un sistema de información o en una tecnología de información, será reprimido con pena privativa de libertad no menor de uno ni mayor de tres años.

La pena será no menor de tres ni mayor de seis si, como consecuencia de los hechos anteriores, resultase un perjuicio para el titular de la data o información, o para un tercero.

Artículo 9.- Violación del secreto de las comunicaciones

El que, mediante el uso de tecnologías de información, acceda, capture, intercepte, interfiera, reproduzca, modifique, desvíe o elimine cualquier mensaje de datos o señal de transmisión o comunicaciones ajenas, será reprimido con pena privativa de libertad no menor de dos ni mayor de cinco años.

Artículo 10.- Revelación indebida de data o información de carácter personal

El que revele, difunda o ceda, en todo o en parte, los hechos descubiertos, las imágenes, el audio o, en general, la data o información obtenidos mediante alguna de las formas indicadas en los dos artículos precedentes, será reprimido con pena privativa de la libertad no menor de uno ni mayor de tres años, aun cuando no hubiese tornado parte en la comisión de dichos delitos.

Si la revelación, difusión o cesión se hubieren realizado con un fin de lucro o si resultare algún perjuicio para otro la pena se aumentará a no menor de tres ni mayor de seis años.

(...)

Capítulo VIII

Disposiciones comunes

Artículo 23.- Agravantes

La pena correspondiente a los delitos previstos en la presente Ley e inclusive a sus agravantes, se incrementará en un tercio por encima del marco penal máximo en los siguientes casos:

1. Si el interviniente comete el delito en calidad de integrante de una organización ilícita dedicada a este tipo de delitos.
2. Si el delito es cometido mediante el abuso de una posición especial de acceso a la data o información reservada o al conocimiento privilegiado de contraseñas en razón del ejercicio de un cargo o función

Disposiciones finales

Primera.- Deróguese el inciso 3, del segundo párrafo del artículo 186, y los artículos 207-A, 207-B y 207-C del Código Penal.

Segunda.- La presente ley entra en vigencia a un mes de su publicación en el Diario Oficial.

10.14.2. Exposición de motivos

Véase el texto completo de esta exposición de motivos en el siguiente enlace:	

10.14.3. Comentarios

El proyecto de Ley N.º 34/2011-CR integra el grupo de iniciativas legislativas que, muy poco tiempo después, originarían la LDI. De este modo, como ya se ha dicho, estamos frente a uno de los principales proyectos legislativos en lucha contra la ciberdelincuencia. A continuación, destacaré algunas ideas centrales:

- Se propuso un cuerpo normativo independiente, es decir, que el marco normativo no actualice el Código Penal, sino que se regule en una ley especial. Los fundamentos para esta decisión fueron tres: (1) la informática ostenta un nivel de tecnicismo o especialización que justifica su tratamiento separado del resto del ordenamiento; (2) la codificación en una ley especial permitiría realizar cambios específicos en tanto la tecnología evoluciona rápidamente; (3) una ley especial permite identificar y establecer normas procesales para la investigación de este tipo de delitos.
- Se recomendó incluir una norma que estableciera el *objeto de la ley*. Si bien la LDI sí la incluyó, no fue en los términos sugeridos, pues el proyecto apuntaba a prevenir y sancionar las conductas que afectasen la *confianza en la informática*, mientras que, en la LDI, se utiliza una fórmula genérica, esto es, reprimir las conductas que afectan *los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal.*

- Se sugirió incluir un apartado de seis términos que permitiesen dotar de contenido a los términos más utilizados en la legislación propuesta -entre ellos, *data* o *información*, *sistema de información*, *tecnología de información*-. La LDI recogió la sugerencia, pero únicamente adoptó dos términos, siguiendo los lineamientos del Convenio de Budapest: *sistema* y *datos informáticos*.
- Se propuso agrupar cinco delitos bajo un capítulo que se hubiese denominado «Delitos contra los sistemas de información y las Tecnologías de Información». Este título difiere del que finalmente se aprobó: «Delitos contra datos y sistemas informáticos».
- La lista de los delitos vinculados a la seguridad informática lleva denominaciones técnicamente correctas -aunque distintas a las que finalmente fueron aprobadas-: (1) intrusismo informático, (2) sabotaje informático, (3) intrusismo o sabotaje de sistemas o tecnologías de información con medidas de seguridad o con información especial, (4) prestación de equipos y servicios con fines de intrusismo y/o sabotaje, y (5) espionaje informático.
- Si bien se propuso incluir un capítulo denominado «Delitos informáticos contra la intimidad y el secreto de las comunicaciones», la interceptación de datos informáticos o, como el proyecto de ley lo denominaba, el *espionaje informático* se regulaba en el capítulo que incluía el resto de los delitos contra la seguridad informática. Lamentablemente, este extremo del proyecto de ley fue modificado y se cambió de ubicación.
- Se recomendó que el delito de abuso de dispositivos informáticos o *prestación de equipos y servicios con fines de intrusismo y/o sabotaje* -en los términos del proyecto-, se ubicase junto al resto de delitos que integran el conjunto de ilícitos que lesionan la seguridad informática. Sin razones técnicas, finalmente, se decidió cambiar su ubicación al capítulo denominado «Disposiciones comunes».
- Se propusieron únicamente dos circunstancias agravantes, las cuales fueron aceptadas: (1) integrar una organización criminal y (2) abusar del conocimiento adquirido en una posición de ventaja, esto es, un *insider*.

- La exposición de motivos menciona la legislación de Estados Unidos, Alemania, Austria, Gran Bretaña, Holanda, Francia, España, Chile y Argentina. Esto permite comprender el interés y el esfuerzo de la comunidad internacional para enfrentar este fenómeno delictivo.
- El proyecto de ley recoge algunas iniciativas legislativas presentadas en periodos previos. Así, por ejemplo, al proponer la represión de los delitos contra la seguridad informática se emplean, con ligeras modificaciones, las fórmulas propuestas años atrás en el proyecto de Ley N.º 1318/2006-CR.

A nivel de tipificación, el primer delito propuesto fue el *intrusismo informático*. En este caso, si bien no se incluyó el elemento *medidas de seguridad*, sí se agregó la expresión *sin la debida autorización*. De otro lado, es importante notar que se propuso sancionar el acceso, interceptación e interferencia de un sistema, dejándose de lado la modalidad conocida como *exceso de autorización*.

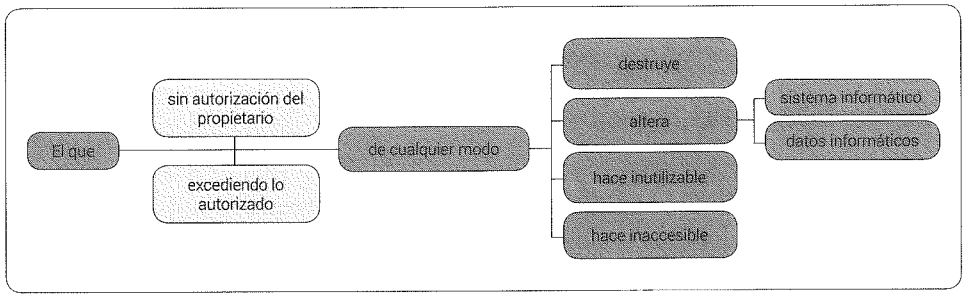


Diagrama 42. Estructura del delito de intrusismo informático, propuesto en el PL N.º 34/2011-CR. Elaboración propia.

El segundo delito, denominado *sabotaje informático*, propuesto en el proyecto de ley recoge dos ilícitos: los ataques contra los sistemas y los datos informáticos. Como se ha señalado líneas arriba, incluye la fórmula que vimos en el proyecto de Ley N.º 1318/2006-CR:

- Se recogen dos modalidades, según el objeto del delito: sistemas informáticos (sistema de información o tecnología de información) o datos informáticos (data o información).
- Se precisa una sanción mayor cuando se utilizan virus o *malware* dado su alto nivel de infestación.

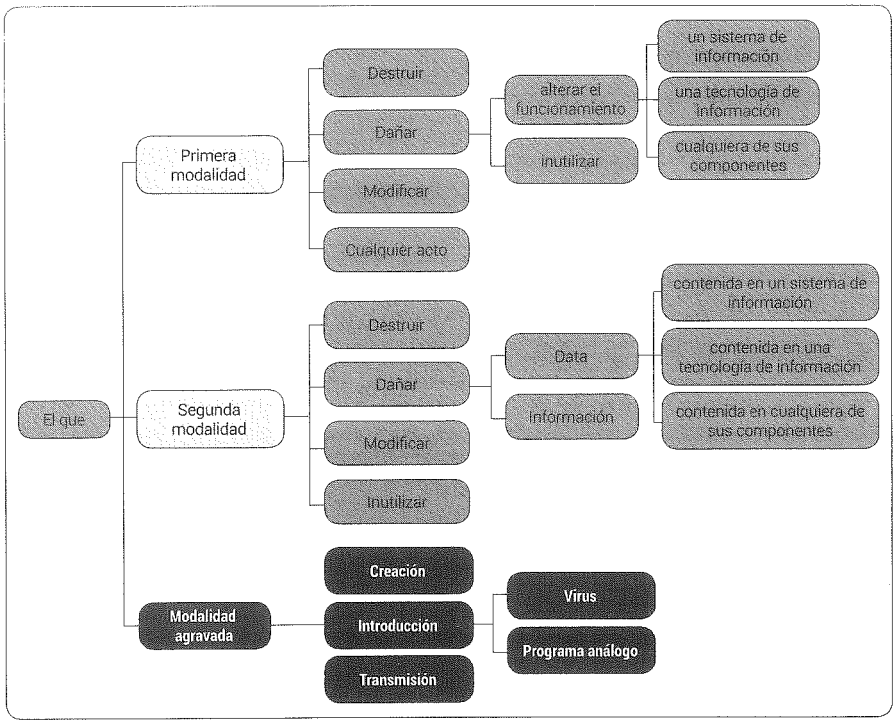


Diagrama 43. Estructura del delito de sabotaje informático, propuesto en el PL N.º 34/2011-CR. Elaboración propia.

El tercer delito que recoge el proyecto de ley analizado sanciona la *prestación de equipos y servicios con fines de intrusismo y/o sabotaje* -lo que, finalmente, se denominaría abuso de dispositivos y mecanismos informáticos-. La fórmula recoge la propuesta desarrollada años atrás en el proyecto de Ley N.º 1318/2006-CR, presentándose los mismos problemas en la tipificación: (1) se sanciona el mero ofrecimiento de los servicios, anticipándose en demasía la represión estatal y (2) se castiga la posesión de elementos que afecten los sistemas o tecnologías de información. De otro lado, se recogen verbos rectores adicionales que no se encontraban sugeridos en el Convenio de Budapest -lo que fue analizado en el capítulo correspondiente de este libro-.

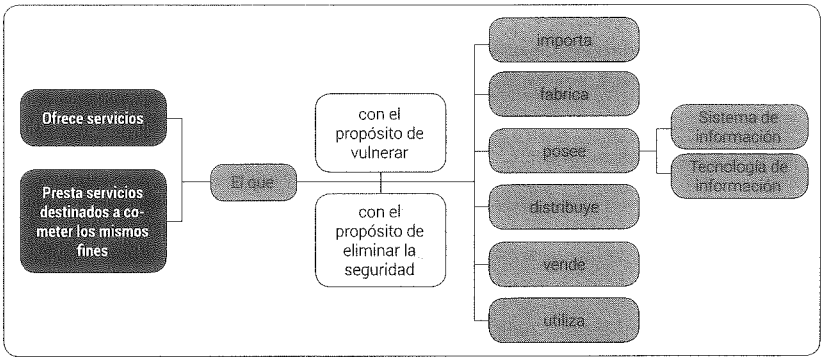


Diagrama 44. Estructura del delito de prestación de equipos y servicios con fines de intrusismo y/o sabotaje, propuesto en el PL N.º 34/2011-CR. Elaboración propia.

El proyecto de ley también recomienda sancionar el *espionaje informático,* esto es, la obtención, revelación o difusión de información contenida en sistemas informáticos. Aunado a ello, se propone incluir dos modalidades agravadas: (1) cuando el delito sea cometido con la finalidad de obtener un beneficio económico y (2) cuando se ponga en riesgo la seguridad del Estado, la confiabilidad de las operaciones financieras o administrativas de las instituciones públicas o privadas, o si resultase algún daño relevante para las personas -sean naturales o jurídicas-. De estas figuras agravadas, solo se recogió íntegramente la primera, en el artículo 11 LDI, y parcialmente la segunda, como modalidad del delito previsto en el artículo 7 LDI.

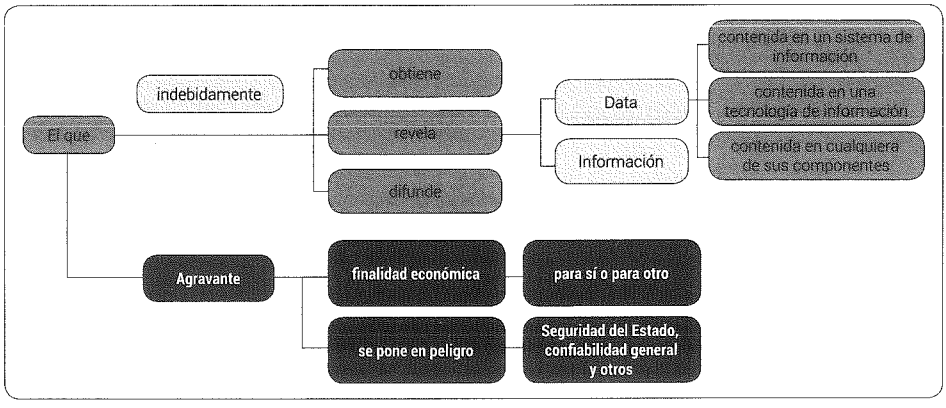


Diagrama 45. Estructura del delito de espionaje informático, propuesto en el PL N.º 34/2011-CR. Elaboración propia.

Como se ha destacado líneas arriba, este es uno de los proyectos de ley más importantes en la historia legislativa peruana en lo que a la lucha contra la cibercriminalidad se refiere.

10.15. PROYECTO DE LEY N.º 307/2011-CR, LEY ESPECIAL SOBRE DELITOS COMETIDOS CON EL USO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

Fecha de presentación: 05 de octubre de 2011

Congresista proponente: Octavio Salazar Miranda

10.15.1. Fórmula legal

Ley especial sobre delitos cometidos con el uso de las tecnologías de la información y comunicaciones

Título Único

Artículo 1.- Objeto

La presente ley tiene por objeto la protección integral de los sistemas que utilicen tecnologías de información, definir nuevas figuras delictivas, definir algunos alcances sobre el Secreto de las Comunicaciones y Secreto Bancario, con la finalidad de facilitar el acceso de la información y otorgar facultades a la Policía Nacional del Perú y Ministerio Público durante la investigación de hechos delictuosos, para la lucha contra el crimen organizado y otros, cometidos con la tecnología de la información y comunicaciones.

Artículo 2.- Comercialización o difusión de base de datos

El que sin tener autorización, ofrezca, venda, intercambie, envíe, difunda, compre, intercepte, modifique, destruya, introduzca virus informáticos o emplee información de carácter personal contenida en ficheros, archivos, bases de datos o medios informáticos, electrónicos o telemáticos, será reprimido con pena privativa de la libertad no menor de dos ni mayor de cuatro años.

Artículo 3.- Prestación de servicios para sabotaje informático

El que sin estar facultado o autorizada para ello, posea, distribuya, diseñe, desarrolle, venda, ejecute, programas o envíe páginas electrónicas, enlaces o ventanas emergentes con el objeto de conseguir valores, bienes, dinero u otros fines ilícitos, será sancionado con pena privativa de libertad no menor de tres ni mayor de seis años.

Artículo 4.- Posesión de equipos de sabotaje informático

El que sin estar autorizada para emitir, fabricar o distribuir tarjetas magnéticas, electrónicas o inteligentes, o instrumentos análogos, re-

ciba, adquiera, posea, transfiera, comercialice, distribuya, venda, controle o custodie cualquier equipo de fabricación de las citadas tarjetas, o de instrumentos destinados a los mismos fines o cualquier equipo o componente que capture, grabe, copie o transmita la data o información que contengan, será sancionado con pena privativa de la libertad no menor de dos ni mayor de cuatro años.

(...)

Artículo 10.- Delitos agravados por el uso de las TICs

El juez podrá elevar la pena hasta la mitad por encima del máximo fijado para el delito cometido, si el agente para cometer o facilitar la comisión del ilícito penal, utiliza o emplea, software o hardware u otras herramientas de la tecnología de la información y comunicaciones. Esta sanción no se aplicará si esta circunstancia se encuentra prevista en el tipo penal.

Disposiciones finales

Primera.- Modificación del art. 207-C del Código Penal

Modifíquese el artículo 207-C del Código Penal el mismo que quedará redactado en los términos siguientes:

Artículo 207-C: Circunstancias agravantes

En los casos de los artículos 207-A y 207-B, la pena será privativa de la libertad no menor de cinco ni mayor de ocho años cuando:

a. Se cometa, haciendo uso de información privilegiada, obtenida en función de su cargo.
b. Las conductas atenten contra instituciones públicas, servicios públicos esenciales, entidades financieras o contra la seguridad nacional

10.15.2. Exposición de motivos

Véase el texto completo de esta exposición de motivos en el siguiente enlace:



10.15.3. Comentarios

Este proyecto de ley aborda principalmente las medidas de investigación tecnológica para luchar eficazmente contra la ciberdelincuencia. De este modo, aunque no es objeto de esta publicación, es importante resaltar que es

en este proyecto de ley en el que se propone incorporar la figura del agente encubierto informático -aunque con facultades distintas a las que finalmente fueron concedidas-.

En el ámbito de la protección penal, el proyecto de Ley N.º 307/2011-CR centra su atención en tres actividades delictivas afines: (1) comercialización o difusión de base de datos, (2) prestación de servicios para sabotaje informático y (3) posesión de equipos de sabotaje informático.

Aunque no fue incorporada como circunstancia agravada de la LDI, en este proyecto de ley se recomendó aumentar la pena cuando la comisión del delito se facilite mediante el uso de *hardware, software* u otra herramienta asociada a las TIC. En este texto hemos graficado e identificado que la mayoría de los ciberdelitos cometidos contra la seguridad informática se cometen por dicho medio. En este sentido, se hubiese sobrecriminalizado las conductas básicas, afectándose, además, el principio de proporcionalidad de la ley penal.

El delito de *comercialización o difusión de base de datos* presenta una estructura confusa, pues de un lado reprime la distribución de virus, pero, simultáneamente, sanciona la comercialización de bases de datos. Esta reunión no responde a criterios técnicos.

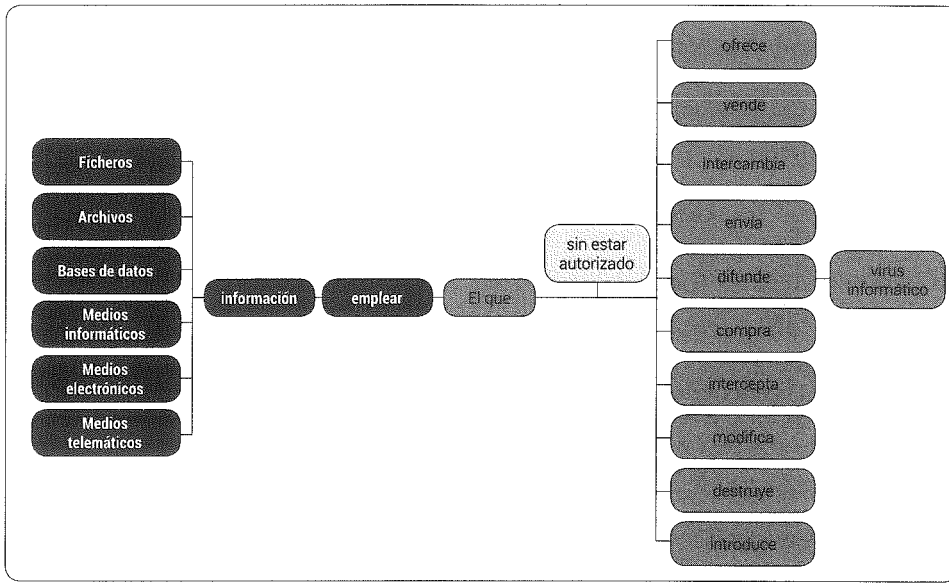


Diagrama 46. Estructura del delito de comercialización o difusión de base de datos, propuesto en el PL N.º 307/2011-CR. Elaboración propia.

Los delitos de *prestación de servicios para sabotaje informático* y de *posesión de equipos de sabotaje informático* sancionan conductas similares. El primero de ellos castiga todo el proceso de producción de páginas maliciosas orientadas a obtener provecho económico ilegal (diseño, desarrollo, venta, ejecución). El segundo sanciona el desarrollo de tarjetas electrónicas, inteligentes o instrumentos similares (*smart cards*) que son destinadas a fines ilegales. De este modo, el legislador intentó cubrir todo espacio que podría ser aprovechado por los ciberdelincuentes.

Finalmente, el proyecto de ley propuso adicionar dos circunstancias agravantes a los delitos recogidos en los artículos 207-B y 207-C CP: (1) acciones cometidas por *insiders* y (2) actos que atentan contra la seguridad nacional, las instituciones públicas, los servicios públicos esenciales y las entidades financieras.

10.16. PROYECTO DE LEY N.º 1136/2011-CR, LEY QUE MODIFICA EL ART. 207-C DEL CÓDIGO PENAL, INCORPORANDO EL DELITO DE ROBO DE IDENTIDAD VIRTUAL E INCORPORA EL ART. 207-D, DELITO INFORMÁTICO AGRAVADO

Fecha de presentación: 17 de mayo de 2012

Congresista proponente: Tomás Zamudio Briceño

10.16.1. Fórmula legal

Ley que modifica el artículo 207-C del Código Penal incorporando el delito de robo de identidad virtual, e incorpora el artículo 207-D, delito informático agravado

(...) Artículo 2.- Incorpórese el art. 207-D del Código Penal, conforme al siguiente texto:

Artículo 207-D. Delito informático agravado

En los casos de los artículos 207-A, 207-B y 207-C, la pena será privativa de libertad no menor de cinco ni mayor de siete años, cuando:

1. El agente accede a una base de datos, sistema o red de computadora, haciendo uso de información privilegiada, obtenida en función a su cargo.

2. El agente pone en peligro la seguridad nacional.

(...)

10.16.2. Exposición de motivos

Véase el texto completo de esta exposición de motivos en el siguiente enlace:	

10.16.3. Comentarios

El objetivo central de este proyecto de ley giró en torno al delito de suplantación de identidad (art. 9 LDI), denominado *robo de identidad virtual* en la propuesta legislativa.

Lo relevante, a efectos de los delitos cometidos contra la seguridad informática, yace en las circunstancias agravantes que se recomendaron incluir: (1) acciones cometidas por *insiders* y (2) cuando los ataques ponen en peligro la seguridad nacional. Este último elemento sería incluido en las circunstancias agravantes que la ley de delitos informáticos recogería en el artículo 11.

10.17. PROYECTO DE LEY N.º 1257/2011-CR, LEY QUE AGRAVA LOS DELITOS DE VIOLACIÓN DEL SECRETO DE LAS COMUNICACIONES

Fecha de presentación: 14 de junio de 2012

Congresista proponente: Tomás Zamudio Briceño

10.17.1. Fórmula legal

Ley que agrava los delitos de violación del secreto de las comunicaciones

Artículo 1.- Objeto de la ley

Incorporar los artículos 161-A, 161-B y 162-A al Código Penal, con la finalidad de agravar los delitos de violación del secreto de las comunicaciones.

Artículo 2.- Modificación del artículo 161 del Código Penal

Incorpórese los artículos 161-A, 161-B del Código Penal, en los términos siguientes:

Artículo 161-A.- La inviolabilidad del secreto de las comunicaciones

Será reprimido con la pena privativa de la libertad no menor de 5 ni mayor de 15 años cuando deliberadamente una persona quien no es el que origina ni es el destinatario de la comunicación, conoce, sustrae, intercepta, interfiere, cambia o altere su texto, desvíe su curso o facilite que terceros conozcan la existencia o contenido de la comunicación.

Tendrán igual sanción las personas que en razón de su función tienen conocimiento o acceso al contenido de una comunicación cursada a través de los servicios públicos de comunicaciones.

(...)

Artículo 3.- Modificación del artículo 162 del Código Penal

Incorpórese el artículo 162-A al Código Penal, en los términos siguientes:

Artículo 162-A. Tenencia ilegal de partes y equipos de interceptación de telecomunicaciones

El que, ilegalmente fabrica, almacena, suministra o tiene en su poder equipo de interceptación de comunicaciones o materiales destinados para su preparación, será reprimido con pena privativa de libertad no menor de 5 ni mayor de 15 años.

La inhabilitación tendrá el mismo plazo que la impuesta por pena privativa de la libertad en caso que el agente activo sea funcionario público y de por vida si es miembro de las Fuerzas Armadas o Policiales.

(...)

10.17.2. Exposición de motivos

Véase el texto completo de esta exposición de motivos en el siguiente enlace:



10.17.3. Comentarios

En la exposición de motivos de este proyecto de ley se registra un suceso histórico ampliamente divulgado en nuestro país en la primera década del siglo XXI: las interceptaciones ilegales de comunicaciones dirigidas contra políticos. En este sentido, se rememoran los eventos ocasionados por la empresa Business Track -cuyos integrantes, finalmente, serían sentenciados-.

En esta publicación, se ha cuestionado la incorporación del delito de interceptación ilegal de datos informáticos (art. 7 LDI) al capítulo de los "Delitos informáticos contra la intimidad y el secreto de las comunicaciones". En este proyecto de ley encontramos uno de los orígenes de los vaivenes del legislador peruano: ¿incorporar las interceptaciones de las comunicaciones en la LDI o en el CP? Como ha demostrado nuestra historia y evolución legislativa, la respuesta del legislador fue inadecuada: reunir tanto el tráfico ilegal de datos como la interceptación de datos informáticos cuando no comparten características similares.

Pocos meses después de la promulgación de la LDI, el delito de tráfico ilegal de datos retornó al CP, mientras que la interceptación ilegal de datos se mantuvo en la LDI, aunque en un capítulo inadecuado.

10.18. PROYECTO DE LEY N.º 2129/2012-CR, LEY QUE SANCIONA LA VENTA ILEGAL DE BASES DE DATOS Y DATOS PERSONALES DE USUARIOS Y CONSUMIDORES

Fecha de presentación: 16 de abril de 2013

Congresista proponente: Jaime Delgado Zegarra

10.18.1. Fórmula legal

Ley que sanciona la venta ilegal de base de datos y datos personales de usuarios y consumidores

Artículo 1. Objeto de la ley

El objeto de la presente ley es incorporar la venta ilegal de base de datos y datos personales de usuarios y consumidores dentro de los delitos informáticos, con el fin de proteger la información concerniente a una

persona física, identificada o identificable, para cuya difusión y/o comercialización no se ha dado autorización.

Artículo 2. Modificatoria

Agréguese el artículo 207-D al Código Penal, aprobado mediante Decreto Legislativo N.º 635, que establece penalizar la venta ilegal de base de datos y datos personales de usuarios y consumidores, en los siguientes términos:

Artículo 207-D. Venta ilegal de base de datos

El agente que utiliza con la finalidad de comercializar, traficar, vender, promover, favorecer o facilitar, información contenida en una base de datos sobre una persona física, identificada o identificable, sin su autorización, relativa a su origen étnico o racial, o que esté referida a sus características físicas, morales o emocionales, a su vida afectiva, familiar, a su domicilio, números telefónicos, patrimonio, situación financiera, laboral o tributaria, o su estado de salud física o mental, o a su ideología y opiniones políticas, creencias o convicciones religiosas o filosóficas; será reprimido con pena privativa de libertad no menor dos ni mayor de cinco años.

10.18.2. Exposición de motivos

Véase el texto completo de esta exposición de motivos en el siguiente enlace:



10.18.3. Comentarios

Al igual que el proyecto de Ley N.º 1257/2011-CR, en este se recomienda sancionar el tráfico ilegal de bases de datos y datos de usuarios y consumidores. Si bien la propuesta legislativa data de abril del 2013, los principales lugares donde esta ilícita actividad se realiza se encontraban plenamente identificados: la avenida Wilson, el centro comercial Polvos Azules y la avenida Argentina.

La propuesta sanciona a quien utiliza información personal, sin autorización alguna:

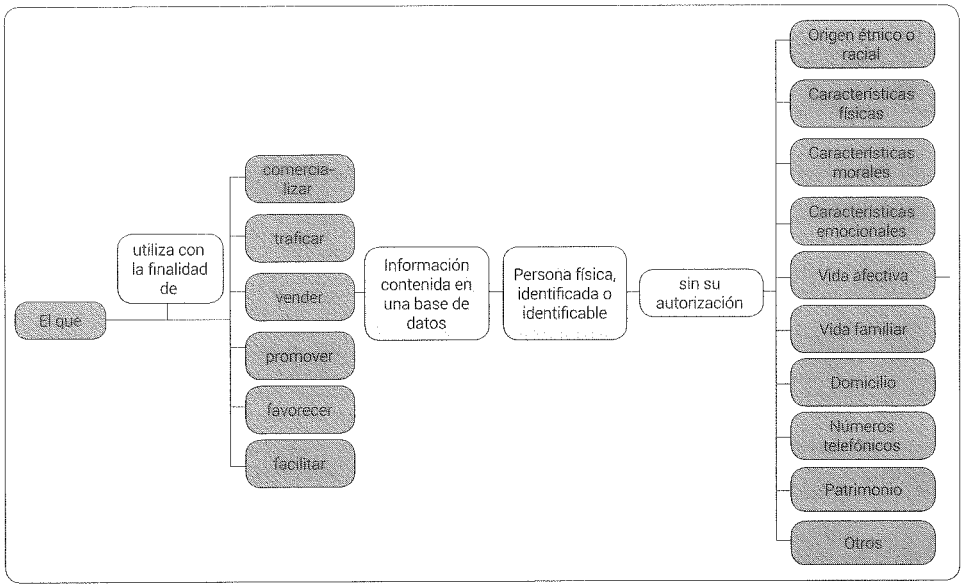


Diagrama 47. Estructura del delito de venta ilegal de base de datos y datos personales de usuarios y consumidores, propuesto en el PL N.º 2129/2012-CR. Elaboración propia.

Esta propuesta legislativa, con algunos cambios, finalmente sería aprobada e ingresaría a la LDI bajo el nombre de *tráfico ilegal de datos* (art. 6). Sin embargo, como se señaló líneas arriba, cinco meses después sería reubicado, dejando la LDI para ingresar al CP. En efecto, este delito no afecta la seguridad informática, sino la intimidad y privacidad personal.

10.19. PROYECTO DE LEY N.º 2520/2012-PE, LEY DE REPRESIÓN DE LA CIBERCRIMINALIDAD

Fecha de presentación: 26 de julio de 2013

Proponente: Poder Ejecutivo, presidente Ollanta Humala Tasso

10.19.1. Fórmula legal

Ley de represión de la cibercriminalidad

Artículo 1.- Objeto

La presente ley tiene por objeto modificar el Código Penal con la finalidad de modernizar la legislación penal en el marco de la lucha eficaz contra la cibercriminalidad.

Artículo 2.- Incorporación del Título V-A del Libro Segundo al Código Penal

Incorpórese el Título V-A al Libro Segundo del Código Penal, el cual tendrá la siguiente composición:

Título V-A: Delitos contra los datos y sistemas informáticos

Capítulo I

Acceso Ilícito

Artículo 208-A.- Acceso ilícito

El que accede sin autorización a todo o parte de un sistema informático siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días multa.

Será reprimido con la misma pena el que accede a un sistema informático excediendo lo autorizado.

Capítulo II

Atentados contra datos y sistemas informáticos

Artículo 208-B.- Atentados a la integridad de datos informáticos

El que, a través de las tecnologías de la información o de la comunicación, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y ochenta a ciento veinte días multa.

Artículo 208-C.- Atentados a la integridad de sistemas informáticos

El que, a través de las tecnologías de la información o de la comunicación, inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa.

Capítulo III

Abuso de dispositivos

Artículo 208-D.- Abuso de mecanismos y dispositivos informáticos

El que fabrica, vende, facilita, distribuye u obtiene para su utilización mecanismos, dispositivos, contraseñas o códigos de acceso específica-

mente diseñados para la comisión de los delitos previstos en los artículos 197-A, 208-A, 208-B, 208-C y 438-A o el que ofrece o presta servicios que contribuya a ese propósito será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días multa.

Capítulo IV

Formas agravadas

Artículo 208-E.- Formas agravadas

En los casos de los artículos 208-A, 208-B y 208-C, el juez podrá aumentar la pena privativa de libertad hasta en un tercio por encima de máximo legal fijado para los tipos penales cuando:

1. El agente comete el delito mediante el abuso de una posición especial de acceso a la data o a información reservada o al conocimiento privilegiado de esta información en razón del ejercicio de un cargo o función.
2. El delito compromete fines asistenciales, la defensa, seguridad o soberanía nacionales.
3. El agente comete el delito con el fin de obtener un beneficio económico.

Artículo 3.- Incorporación de los artículos 162-A, 183-B, 197-A y 438-A al Código Penal

Incorpórese los artículos 162-A, 183-B, 197-A y 438-A al Código Penal, en los siguientes términos.

Artículo 162-A.- Interceptación de datos informáticos

El que, a través de las tecnologías de la información o de la comunicación, intercepta datos informáticos en transmisiones no públicas, dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos, será reprimido con una pena privativa de libertad no menor de tres ni mayor de seis años.

La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con las normas de la materia.

La pena privativa de libertad será no menor de ocho ni mayor de diez años cuando el delito comprometa la defensa, seguridad o soberanía nacionales.

(...)

Disposiciones complementarias finales

Primera.- Convenios Multilaterales

El Estado peruano promoverá la firma y ratificación de convenios multilaterales que garanticen la cooperación mutua con otros Estados para la persecución de la cibercriminalidad.

Segunda.- Terminología

Para los efectos de la presente ley, se entenderá, conforme al artículo 1 del Convenio sobre la Ciberdelincuencia, Budapest, 23.XI.2001:

a) **Por sistema informático:** todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa.

b) **Por datos informáticos:** toda representación de hechos, información o conceptos, expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función.

(...)

10.19.2. Exposición de motivos

Véase el texto completo de esta exposición de motivos en el siguiente enlace:



10.19.3. Comentarios

Este proyecto de ley, elaborado por el Poder Ejecutivo bajo la dirección del presidente Ollanta Humala, fue el último recibido por el Congreso de la República antes de la discusión y el debate previo a la aprobación y promulgación de la LDI. Sin lugar a duda, junto al proyecto elaborado por el congresista Eguren Neuenschwander son los que mayor influencia e impacto tuvieron en la legislación aprobada.

Este proyecto se encuentra muy bien articulado y utiliza correctamente la terminología, desde el plano técnico y jurídico, además de advertirse una clara influencia del Convenio de Budapest en su redacción –al cual se refiere expresamente en el acápite denominado *Expansión de la cibercriminalidad*–.

De este modo, por ejemplo, en esta propuesta legislativa se resalta la importancia de los ataques ejecutados mediante ingeniería social. En este libro, hemos abordado diferentes casos que grafican su impacto para facilitar la comisión de varios ilícitos; sin embargo, es importante resaltar que la ingeniería social se utiliza no solo para cometer delitos contra el patrimonio o la libertad e indemnidad sexual –aunque son los más frecuentes o conocidos–, sino también para realizar ataques contra la seguridad informática. Temperini y Macedo lo grafican en los siguientes términos:

> a) Ataques de ingeniería social que afectan la disponibilidad
>
> Podemos enunciar aquellos intentos de incitar a que la víctima que realice o deje de hacer una acción que imposibilite el acceso de los usuarios legítimos. Un ejemplo sería que un usuario, al que se lo convence de que se realizarán tareas de mantenimiento en la zona con peligro para las instalaciones eléctricas, corta el sistema de energía eléctrica, imposibilitando la prestación de un determinado servicio.
>
> b) Ataques de ingeniería social que afectan la integridad
>
> Referimos aquellos supuestos en los cuales se incita a que la víctima realice una acción que permita insertar un registro de información, que de otra forma no lo hubiese realizado. Un ejemplo sería una llamada telefónica, haciéndose pasar por el titular de una cuenta, logrando cambiar el correo electrónico asociado a un usuario, que posteriormente permitiría otro tipo de ataques.
>
> c) Ataques de ingeniería social que afectan la confidencialidad
>
> Podemos enunciar aquellos intentos de incitar a que la víctima permita el acceso a la información confidencial que de otra forma no se hubiese logrado. Un ejemplo sería el caso de quien se contacta con un gerente, haciéndose pasar por personal técnico de la empresa, y duran-

> te el contacto logra que le brinde el usuario y contraseña que utiliza para el sistema operativo[895].

Este proyecto de ley, de un lado, recoge estadística valiosa y, de otro, resalta la variedad de tipos de ataques y cibercriminales que convergen en las redes. Así, por ejemplo, se resalta que, al 2013, Colombia, Brasil, Ecuador, Perú, Venezuela y Bolivia son los países con más incidencia de la región sudamericana en lo que a crecimiento de la ciberdelincuencia se refiere. Esto explica la preocupación de los Poderes Legislativo y Ejecutivo por legislar de forma adecuada y, de algún modo, enfrentar tan novedoso fenómeno delictivo. En esta línea, se destaca que Perú, después de Brasil, es el segundo país fuente de desarrollo de *malware* y *crimeware* de la región.

Al explicar las razones de la tipificación, la propuesta legislativa se posiciona como un marco normativo de vanguardia al reconocer que se busca proteger tanto los sistemas informáticos como los datos que estos contienen. Es más, expresamente se señala que la legislación no solo debe proteger bienes tradicionales, sino estas nuevas expresiones –erigiéndose, de este modo, como pauta interpretativa de los alcances y límites de los tipos penales–:

> Los tipos penales que pretende incorporar esta iniciativa lesionan o ponen en peligro diversos bienes jurídicos. Por un lado, se muestran peligrosos frente a bienes jurídicos tradicionales (el patrimonio, la libertad sexual, la fe pública, la intimidad personal, la seguridad nacional o la propiedad intelectual); y por otro, **los sistemas y datos informáticos como bienes jurídicos en sí mismos** (...) [El resaltado es mío]

Si bien el proyecto no sugiere adoptar una ley especial, sí recomienda crear un capítulo específico que recoja cuatro delitos dirigidos contra los sistemas y datos informáticos –lo que en este libro se ha denominado *ataques contra la seguridad informática*–.

895 Temperini, Marcelo y Maximiliano Macedo. "Aspectos legales de la ingeniería social: Análisis de la responsabilidad civil y penal del ingeniero social". En: Riquert, Marcelo A. (dir.) y Carlos Christian Sueiro (coord.). *Sistema penal e informática. Ciberdelitos. Evidencia digital. TICS*, vol. 3. Buenos Aires: Hammurabi, 2020, p. 71.

a) Acceso ilícito: propone sancionar tanto el acceso con ruptura de medidas de seguridad como el exceso en la autorización. Esta fórmula no incluye los elementos deliberada ni ilegítimamente.

b) Atentado a la integridad de datos informáticos: precisa que el medio de ataque son las TIC. Además, incluye un verbo rector no sugerido en el Convenio de Budapest: introducir datos informáticos.

c) Atentado a la integridad de sistemas informáticos: sugiere sancionar la inutilización de un sistema informático, impedir el acceso, entorpecer su funcionamiento o imposibilitar la prestación de sus servicios. Lamentablemente, no se incluyó el elemento *gravedad* que permita distinguir la trascendencia o nivel de impacto del evento.

d) Interceptación de datos informáticos: la fórmula legislativa es afín a la que finalmente fue aprobada.

Finalmente, es importante destacar que este proyecto de ley recomendó tres de las cuatro circunstancias que finalmente serían adoptadas: (1) cometer el delito como parte de una organización criminal, (2) abusar de la posición o información proporcionada al *insider* y (3) cometer el delito con un propósito económico.

Recomiendo revisar la estadística detallada en la exposición de motivos de este proyecto, en tanto recoge información valiosa que permite viajar en el tiempo y conocer los escenarios bélicos-informáticos a los cuales se debía enfrentar nuestro legislador.

10.20. PROYECTO DE LEY N.º 2991/2013-CR, LEY QUE MODIFICA LA LEY N.º 30096, LEY DE DELITOS INFORMÁTICOS

Fecha de presentación: 25 de noviembre de 2013

Congresista proponente: Juan Carlos Eguren Neuenschwander

10.20.1. Fórmula legal

Ley que modifica la Ley 30096, Ley de Delitos Informáticos

Artículo 1. Modificación de los artículos 2, 3, 4, 7, 8 y 10 de la Ley 30096, Ley de Delitos Informáticos

Modificase los artículos 2, 3, 4, 7, 8 y 10 de la Ley 30096, Ley de Delitos Informáticos, en los siguientes términos:

Artículo 2. Acceso ilícito

El que deliberada e ilegítimamente accede a todo o en parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa.

Será reprimido con la misma pena, el que accede a un sistema informático excediendo lo autorizado.

Artículo 3. Atentado a la integridad de datos informáticos

El que deliberada e ilegítimamente daña, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa.

Artículo 4. Atentado a la integridad de sistemas informáticos

El que deliberada e ilegítimamente inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa.

Artículo 7. Interceptación de datos informáticos

El que deliberada e ilegítimamente intercepta datos informáticos en transmisiones no públicas, dirigidos a un sistema informático, originados en un sistema informático o efectuado dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos, será reprimido con una pena privativa de libertad no menor de tres ni mayor de seis años.

La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con la Ley de transparencia y acceso a la información pública.

La pena privativa de libertad será no menor de ocho ni mayor de diez cuando el delito comprometa la defensa, seguridad o soberanía nacionales.

(...)

Artículo 10. Abuso de mecanismos y dispositivos informáticos

El que deliberada e ilegítimamente fabrica, diseña, desarrolla, vende, facilita, distribuye, importa u obtiene para su utilización, uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la presente Ley, o el que ofrece o presta servicio que contribuya a ese propósito, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días- multa."

Artículo 2. Incorporación del artículo 12 a la Ley 30096, Ley de delitos informáticos. Incorpórase el artículo 12 a la Ley 30096, Ley de delitos informáticos, en los siguientes términos:

Artículo 12. Exención de responsabilidad penal

Está exento de responsabilidad penal el que realiza las conductas descritas en los artículos 2, 3, 4 y 10 con el propósito de llevar a cabo pruebas autorizadas u otros procedimientos autorizados destinados a proteger sistemas informáticos.

(...)

10.20.2. Exposición de motivos

Véase el texto completo de esta exposición de motivos en el siguiente enlace:	

10.20.3. Comentarios

A fines de octubre del 2013, se publicó la LDI. Un mes después, nuestros legisladores ya exigían un cambio. Uno de los argumentos centrales –común a los proyectos de ley que se analizarán a continuación– fue que la tipificación no sería *acorde* al Convenio de Budapest, porque no se incluyó la fórmula original. Esto es, no se agregaron los elementos *deliberada e ilegítimamente* en los tipos penales de acceso ilícito, atentado contra datos y sistemas informáticos, entre otros ilícitos. Lamentablemente, el legislador pensó que el Convenio así lo exigía cuando no es así. El profesor argentino Marcelo Riquert, a fines del 2014, así lo puntualizaba:

> Al iniciar el trabajo de comparación normativa resulta conveniente recordar que el Convenio de Budapest no provee una "redacción tipo" de delitos cual suerte de receta inalterable, sino una formulación genérica, abierta y, en algunos casos, con la sugerencia de alternativas para que los signatarios puedan adaptar conforme a su propio diseño de derecho local.
>
> Esta característica, lógica y apropiada para lo que resulta una suerte de marco referencial, dificulta el cotejo con la regulación nacional, ya que dentro del universo de casos en consideración hay legislación pre-convenio y post-convenio, de países que lo han firmado u otros que no, que han realizado una tipificación más amplia o más restrictiva y, a la vez, que lo hicieron en forma más concentrada o más dispersa en un doble sentido:
>
> a) En cuanto a la adopción de una ley especial o un capítulo específico en su Código Penal, o en alternadas modificaciones en leyes especiales y el propio Código Penal, o difuminada o sectorizada dentro del último.
>
> b) En cuanto al Convenio, brinda en algún artículo una serie de verbos típicos para los que no hay una sola norma nacional que los reciba juntos, sino que puede hacerlo desperdigados entre diferentes tipicidades o, incluso, solo parcialmente.
>
> Es esencial no perder de vista este factor porque al concretar la comparación tendiente a establecer asertiva o negativamente la recepción de una propuesta en el nivel nacional, en ocasiones se improvisa una respuesta que sería tendencial y no exacta, es decir que puede darse el caso que sin haber correspondencia precisa, aun con algún déficit meno de tipicidad, no puede sostenerse la absoluta laguna de punibilidad y, por eso, se entiende que existe cumplimiento con el requisito externo aunque sea parcial[896].

Además de incluir innecesaria e inadecuadamente los elementos antes mencionados, el legislador peruano propuso incluir el artículo 12 LDI y, de este modo, exonerar de responsabilidad penal a quien cometiese los delitos de acceso ilícito, atentado contra los datos y sistemas informáticos y abuso de

896 Riquert, *Ciberdelitos: Grooming, stalking, bullying, sexting, ciberodio, propiedad intelectual, problemas de perseguibilidad, ciberpornografía infantil*, cit., p. 49 y s.

dispositivos informáticos, pero cuya actuación se realizara con la finalidad de realizar pruebas autorizadas o dirigidas a proteger los equipos informáticos.

10.21. PROYECTO DE LEY N.º 2999/2013-CR, LEY QUE MODIFICA, INCORPORA Y DEROGA DIVERSOS ARTÍCULOS A LA LEY N.º 30096, LEY DE DELITOS INFORMÁTICOS

Fecha de presentación: 27 de noviembre de 2013

Congresista proponente: Mauricio Mulder Bedoya

10.21.1. Fórmula legal

Ley que promueve modificar los artículos 2, 3, 4, 5, 7, 9, 10; lo mismo en la tercera y cuarta disposición complementaria final y en la cuarta disposición complementaria modificatoria en su artículo 162 CP y derogatoria de los artículos 6 y 8 de la Ley 30096, Ley de Delitos Informáticos

Artículo primero.- Modificar los artículos 2, 3, 4, 5, 7, 9 y 10 de la Ley N.º 30096, "Ley de Delitos Informáticos".

Los artículos deben decir lo siguiente:

Artículo 2.- Acceso ilícito

El que accede de manera deliberada e ilegítima a todo o en parte de un sistema informático, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa.

Será reprimido con pena privativa de la libertad de tres a cinco años y con noventa días-multa siempre que el delito se realice con vulneración de medidas de seguridad establecidas para impedirlo.

Artículo 3.- Atentado a la integridad de datos informáticos

El que de manera deliberada e ilegítima, dañe, borre, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con pena privativa de libertad no menor de Tres ni mayor de seis años y con ochenta a ciento veinte días-multa.

Artículo 4.- Atentado a la integridad de sistemas informáticos

El que de manera deliberada e ilegítima afecte el funcionamiento de un sistema informático mediante la introducción, transmisión, daño,

borrado, deterioro, alteración o supresión de datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa.

(...)

Artículo 7.-. Interceptación ilícita de datos informáticos

El que, intercepta de manera deliberada e ilegítima, datos informáticos en transmisiones no públicas, dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos, será reprimido con una pena privativa de libertad no menor de tres ni mayor de seis años.

La pena privativa de la libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con las normas de la materia.

(...)

Artículo 10.- Abuso de mecanismos y dispositivos informáticos

El que de manera deliberada e ilegítima, produce, vende, obtiene para su utilización, importa, difunde o pone a disposición, cualquier dispositivo, incluido un programa informático, contraseñas, código de acceso o datos informáticos específicamente diseñados para la comisión de los delitos previstos en la presente Ley o el que ofrece o presta servicio que contribuya a ese propósito, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa.

No se interpretará que el presente artículo impone responsabilidad penal cuando la producción, venta, obtención para la utilización, importación, difusión o cualquiera otra forma de puesta a disposición mencionada en el párrafo 1 del presente artículo no tenga por objeto la comisión de uno de los delitos previstos de conformidad con los artículos de la presente Ley, como en el caso de las pruebas autorizadas o de la protección de un sistema informático

(...)

10.21.2. Exposición de motivos

Véase el texto completo de esta exposición de motivos en el siguiente enlace:	

10.21.3. Comentarios

Dos días después de la presentación del proyecto de Ley N.º 2991/2013, se ingresó una nueva propuesta de reforma normativa. Si bien se recogieron diversas opiniones de expertos en la materia, nuestro legislador no reflexionó sobre las consecuencias jurídico-penales que traería consigo incluir el elemento *deliberadamente* en los tipos penales.

De este modo, bajo la supuesta premisa de que la legislación original nos alejaba de instrumentos internacionales en la lucha contra la ciberdelincuencia como el Convenio de Budapest, se realizaron algunos cambios normativos que limitan, incluso hoy en día, los alcances de los delitos informáticos.

Lamentablemente, la reforma legislativa de inicios del 2014 no estuvo acompañada de un diálogo técnico penal ni del juicio reflexivo que se requería. Las opiniones recogidas en la exposición de motivos reflejan genuino interés por mejorar la legislación especializada, pero debió acompañarse de un debate mucho más profundo y pausado.

10.22. PROYECTO DE LEY N.º 3105/2013-CR, LEY QUE MODIFICA LA LEY N.º 30096, LEY DE DELITOS INFORMÁTICOS

Fecha de presentación: 18 de diciembre de 2013

Congresista proponente: Carmen Omonte Durand

10.22.1. Fórmula legal

Ley que modifica la Ley N.º 30096, Ley de Delitos Informáticos

Artículo 1.- Modifíquense los artículos 3, 7 y 10 de lo Ley N.º 30096, Ley de Delitos Informáticos, los que quedaron redactados de lo siguiente manera:

Art. 3.- Atentado a la integridad de datos informáticos

El que, de manera ilegítima, o través de las tecnologías de la información o de la comunicación, introduce, borra, deteriora, altera, daña, suprime o hace inaccesibles datos informáticos, será reprimido con pena privativa de identidad no menor de mes ni mayor de seis años y con ochenta a ciento veinte días-multa.

Art. 7.- Interceptación de datos informáticos

El que, a través de los tecnologías de la información o de la comunicación, intercepta datos informáticos en transmisiones no públicas originadas en un sistema informático o efectuados dentro del mismo, incluidos los emisiones electromagnéticos provenientes de un sistema informático que transporte dichos datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años.

La pena privativa de la libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreto, reservada o confidencial, de conformidad con las normas de lo materia.

La pena privativa de libertad será no menor de ocho ni mayor de diez cuando el delito comprometo lo defensa, seguridad o soberanía nacionales.

Art. 10.- Abuso de mecanismos y dispositivos informáticos

El que fabrica, diseña, desarrolla, vende, facilita, distribuye, importa u obtiene para su utilización, uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la presente Ley, o el que ofrece o presta servicio que contribuya a ese propósito, será reprimido con pena privativo de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa.

No son reprimibles la producción, venta, obtención para lo utilización, importación, difusión o cualquiera otra forma de puesta a disposición mencionado en el presente artículo que no tenga por objeto la comisión de uno de los delitos previstos de conformidad con los artículos con los artículos de la presente Ley, como en el caso de las pruebas autorizadas o de lo protección de un sistema informática.

10.22.2. Exposición de motivos

Véase el texto completo de esta exposición de motivos en el siguiente enlace:	

10.22.3. Comentarios

Este proyecto de ley se sumó a las propuestas de modificación dirigidas a homologar los tipos penales previstos en la LDI, a la luz de las recomendaciones del Convenio de Budapest. No obstante, solo se sugirió actualizar tres delitos:

a) Atentado a la integridad de datos informáticos: se recomendó incluir el elemento *de manera ilegítima*. Además, propuso añadir el verbo rector *dañar*.

b) Interceptación de datos informáticos: se sugirió eliminar la interceptación de datos dirigidos a un sistema informático, manteniendo el resto de las modalidades y estructura típica.

c) Abuso de mecanismos y dispositivos informáticos: se propuso incluir un párrafo adicional que exima de responsabilidad penal si las conductas desplegadas tuviesen como objetivo realizar pruebas autorizadas o proteger los sistemas informáticos. Este punto, finalmente, sería acogido como un supuesto de exención de responsabilidad penal (art. 12 LDI).

Esta propuesta legislativa es la última que se recibió antes de promulgar la Ley N.º 30171 de marzo del 2014, norma que modificaría tanto la LDI como algunos artículos del CP. El proyecto de ley presentado por la congresista Martha Chávez –que será revisado a continuación– no fue incluido en el grupo en mención ni aprobado.

10.23. PROYECTO DE LEY N.º 3980/2014-CR, LEY QUE PROPONE MODIFICAR LA LEY N.º 30096, LEY DE DELITOS INFORMÁTICOS, MODIFICADA POR LA LEY N.º 30171

Fecha de presentación: 13 de noviembre de 2014

Congresista proponente: Martha Chávez Cossío

10.23.1. Fórmula legal

Ley que modifica la Ley N.° 30096, Ley de Delitos Informáticos, modificada por Ley N.° 30171

Artículo único.- Modifica los artículos 1 y 10 de la Ley N.° 30096, Ley de Delitos Informáticos, modificada por Ley 30171

Modifícase los artículos 1 y 10 de la Ley N.° 30096, Ley de Delitos Informáticos, modificada por Ley N.° 30171, los que quedarán redactados en los siguientes términos:

Artículo 1. Objeto de la Ley

La presente Ley tiene por objeto prevenir y sancionar las conductas ilícitas que afectan el derecho de propiedad, la protección de los datos personales y la intimidad de las personas contenidos en los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal cometidas mediante la utilización de tecnología de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia.

Artículo 10.- Abuso de mecanismos y dispositivos informáticos

El que deliberada e ilegítimamente fabrica, diseña, desarrolla, vende, facilita, distribuye, importa u obtiene para su utilización, uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la presente Ley, o el que deliberada e ilegítimamente ofrece o presta servicio que contribuya a ese propósito, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días multa.

10.23.2. Exposición de motivos

Véase el texto completo de esta exposición de motivos en el siguiente enlace:

10.23.3. Comentarios

Con la finalidad de aclarar la LDI actualizada al 2014, la congresista Martha Chávez propuso dos cambios que no serían aceptados:

a) Objeto de la ley (art. 1 LDI): se sugirió precisar que el objeto de protección no son los datos o los sistemas informáticos, sino los derechos relacionados a estos –propiedad, protección de datos personales e intimidad–. Este cambio hubiese significado un retroceso en el reconocimiento de la seguridad informática como bien jurídico protegido por la LDI.

b) Abuso de mecanismos y dispositivos informáticos (art. 10 LDI): se recomendó incluir los elementos *deliberada e ilegítimamente* en la segunda modalidad del tipo penal (ofrecer o prestar servicios). La exposición de motivos es sinceramente preocupante, pues se sostiene que "es necesario incluir el dolo para que se configure este tipo penal". Sin embargo, no es así. El artículo 12 CP expresamente señala que "el agente de infracción culposa es punible en los casos expresamente establecidos por la ley". Dicho de otro modo, no es correcto sostener que, si no se menciona expresamente que la conducta es dolosa, el delito reprime también modalidades culposas.

Como se ha señalado, ambas propuestas no fueron técnica ni jurídicamente adecuadas. Su aprobación hubiese generado problemas de interpretación y aplicación.

10.24. PROYECTO DE LEY N.° 5630/2020-CR, LEY DE SEGURIDAD INFORMÁTICA Y REPRESIÓN DE LOS DELITOS INFORMÁTICOS

Fecha de presentación: 25 de junio de 2020

Congresista proponente: Robertina Santillana Paredes

10.24.1. Fórmula legal

Ley de seguridad informática y represión de los delitos informáticos

Capítulo VI

Delitos Informáticos

Artículo 17.- Intrusismo informático

17.1 El que sin contar con autorización o haciendo uso indebido de ella, accede o facilita a otro el acceso al conjunto o una parte de un

sistema informático, o se mantiene en el mismo, con la intención de obtener información, datos informáticos, o con cualquier otra intención delictiva, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con treinta a noventa días-multa.

17.2 La pena privativa de libertad será no menor de seis ni mayor de diez, cuando el intrusismo es cometido abusando de una posición privilegiada de garante o custodio de los datos contenidos en un sistema informático en razón del ejercicio de un cargo o función, o tiene por fin la obtención de un beneficio económico para sí o para tercero.

17.3 La pena privativa de libertad será no menor de ocho ni mayor de quince cuando el delito comprometa la función pública, la acción de la justicia, la defensa, seguridad o soberanía nacionales.

Artículo 18.- Perturbación informática

18.1 El que deliberadamente, valiéndose de cualquier medio, daña, borra, deteriora, altera, suprime, entorpece, hace inaccesible o imposibilita el funcionamiento de un sistema, una red, un programa o datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa.

18.2 La pena privativa de la libertad será no menor de seis ni mayor de diez cuando el delito tiene por fin el sabotaje comercial o industrial, es cometido abusando de una posición privilegiada de garante o custodio de los datos contenidos en un sistema informático, en razón del ejercicio de un cargo o función; o tiene por fin la obtención de un beneficio económico para sí o para tercero.

18.3 La pena privativa de libertad será no menor de ocho ni mayor de quince cuando el delito comprometa la función pública, la acción de la justicia, la defensa, seguridad o soberanía nacionales.

Artículo 19.- Interceptación de datos informáticos

19.1 El que deliberada e ilegalmente intercepta datos informáticos de terceros, en transmisiones no públicas, dirigidos, originados o efectuados dentro de un sistema informático, incluidas las emisiones electromagnéticas que transporten dichos datos informáticos, será reprimido con una pena privativa de libertad no menor de tres ni mayor de seis años.

19.2 La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información personal, comercial o industrial, secreta, reservada o confidencial

19.3 La pena privativa de libertad será no menor de ocho ni mayor de diez cuando el delito comprometa la función pública, la acción de la justicia, la defensa, seguridad o soberanía nacionales.

19.4 Si el agente comete el delito como integrante de una organización criminal, la pena se incrementa hasta en un tercio por encima del máximo legal previsto en los supuestos anteriores.

Artículo 24.- Abuso de mecanismos y dispositivos informáticos

El que deliberada e ilegítimamente fabrica, diseña, desarrolla, vende, facilita, distribuye, importa u obtiene para su utilización, uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la presente Ley, o el que ofrece o presta servicio que contribuya a ese propósito, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa.

(...)

Disposición derogatoria final

Primera.- Derogase la Ley N.º 30096 y su modificación efectuada por Ley N.º 30171 y toda norma que se oponga a lo dispuesto en la presente Ley.

10.24.2. Exposición de motivos

Véase el texto completo de esta exposición de motivos en el siguiente enlace:	

10.24.3. Comentarios

En junio del 2020, casi seis años después de la última propuesta legislativa, se propuso derogar la LDI y, en su reemplazo, adoptar la *Ley de seguridad informática y represión de los delitos informáticos*. Entre los cambios más resaltantes, tenemos los siguientes:

- Se propuso cambiar la denominación de *acceso ilícito* a *intrusismo informático*, incluir la ocupación indebida como nueva modalidad y agravar la pena cuando el ilícito fuese cometido por un *insider*.

- Se recomendó unir los delitos de atentados contra datos y sistemas informáticos bajo un mismo tipo penal denominado *perturbación informática*. A diferencia de otros delitos y sin mayor explicación, se incluyó el elemento *deliberadamente* como parte del tipo penal. Aunado a esto, el objeto del delito no se restringe a datos y sistemas informáticos, pues se amplía a programas y redes.
- Tanto la interceptación de datos informáticos como el abuso de mecanismos y dispositivos informáticos tienen la misma estructura típica que en la LDI. Lamentablemente, se continúa considerando que el *ofrecimiento de servicios* es una conducta penalmente relevante y que debería sancionarse de forma autónoma.

10.25. PROYECTO DE LEY N.º 9136/2024-CR, LEY QUE MODIFICA LA LEY DE DELITOS INFORMÁTICOS RESPECTO A LA ACTIVACIÓN Y POSESIÓN ILEGAL DE SIM CARDS

Fecha de presentación: 9 de octubre de 2024

Congresista proponente: Rosangella Andrea Barbarán Reyes

10.25.1. Fórmula legal

Ley que modifica la Ley 30096, Ley de Delitos Informáticos, respecto a la activación y posesión ilegal de SIM cards

Artículo 1. Incorporación del artículo 10-A en la Ley N.º 30096, Ley de Delitos Informáticos

Se incorpora el artículo 10-A en la Ley N.º 30096, Ley de Delitos Informáticos, en los siguientes términos.

Artículo 10-A.- Activación y posesión ilegal de SIM cards

El que mediante las tecnologías digitales activa uno o más SIMs cards físicos o virtuales, utilizando datos personales o biométricos, sin el consentimiento de su titular será reprimido con pena privativa de libertad no menor de cuatro ni mayor de ocho años y con inhabilitación conforme al numeral 4 del artículo 36 del Código Penal.

La misma pena se aplicará al agente que facilite, adquiere, posee, comercialice uno o más SIMs cards activados ilegalmente o teléfono

móvil con SIM card virtual a sabiendas que se encuentra activados ilegalmente.

Artículo 2. Derogación del artículo 222-B del Decreto Legislativo 635, Código Penal peruano, referido a la posesión ilegítima de SIM cards activados

Se deroga el artículo 222-B del Decreto Legislativo 635, Código Penal peruano, referido a la posesión ilegítima de SIM cars activados.

10.25.2. Exposición de motivos

Véase el texto completo de esta exposición de motivos en el siguiente enlace:	

10.25.3. Comentarios

El 9 de octubre del 2024, se presentó un proyecto de ley que sugirió incorporar la activación y posesión ilegal de SIM *cards* como un nuevo delito informático e incluirlo, de este modo, a la LDI. Como la seguridad ciudadana en Perú se ha visto mermada en los últimos años, el Poder Legislativo impulsó la discusión y debate de proyectos de ley que podrían contrarrestar esta crisis. Es así como, el 10 de abril del 2025, se realizó la primera votación de este proyecto de ley, siendo aprobado y exonerado de una segunda votación. Finalmente, el 16 de abril, se remitió la autógrafa al Poder Ejecutivo para su análisis, aprobación u observación.

En atención a una posible entrada en vigor, es importante destacar algunos comentarios:

- No es un delito informático y, de forma inadecuada, se ubica en la LDI. Es más, ha sido incorporado en el capítulo denominado *Delitos informáticos contra la fe pública*, junto al delito de *suplantación de identidad.*
- El delito debería ser reubicado en el capítulo de *Delitos contra la propiedad industrial* del CP. De este modo, compartiría la misma ubicación que el delito de penalización de la clonación o adulteración de terminales de telecomunicaciones (art. 222-A CP),

posesión ilegítima de SIM cards activados (art. 222-B CP), comercialización de equipos de terminales móviles con IMEI lógico o físico alterado, reemplazado o duplicado (art. 222-C CP) y posesión ilegítima de dispositivos para adulterar, reemplazar, duplicar o modificar IMEI (art. 222-D CP).

- Aunque la activación ilegal de SIM *cards* permita cometer delitos informáticos como la suplantación de identidad, también facilita delitos tradicionales como la extorsión, la trata de personas y la estafa. En consecuencia, no se advierten argumentos que justifiquen su tratamiento como un ciberdelito –y, mucho menos, como uno que vulnere la seguridad informática–.

10.26. PROYECTO DE LEY N.º 9443/2024-CR, LEY QUE PROTEGE A LOS PERUANOS FRENTE A LAS AMENAZAS CIBERNÉTICAS

Fecha de presentación: 6 de noviembre de 2024

Congresista proponente: Esdras Ricardo Medina Minaya

10.26.1. Fórmula legal

Ley que protege a los peruanos frente a las amenazas cibernéticas

Artículo 1. Objeto de la ley

La presente ley tiene como objetivo modificar los artículos 2 y 4 de la Ley de Delitos Informáticos, Ley N.º 30096 para adaptarla a los desafíos actuales en materia de ciberseguridad. Esta modificación busca fortalecer la protección de los ciudadanos frente a las amenazas del cibercrimen, garantizando un marco legal actualizado.

Artículo 2. Finalidad de la ley

La presente ley tiene como finalidad actualizar la normativa vigente para alinearla con las exigencias del Convenio de Budapest, del cual Perú es parte. Este tratado internacional establece estándares que fomenten la cooperación y la armonización de las legislaciones en la lucha contra los delitos informáticos. Al adoptar estas normas, podremos mejorar nuestras capacidades de respuesta ante incidentes de ciberseguridad, fortaleciendo así la protección de nuestros ciudadanos en el entorno digital.

Artículo 3. Modificación del artículo 2y 4 de la Ley de Delitos Informáticos, Ley N.° 30096

Modifíquese el artículo 2 y 4 de la Ley de Delitos Informáticos Ley N.° 30096 bajo los siguientes términos:

Artículo 2. Acceso ilícito

El que deliberada e ilegítimamente accede a todo o en parte de un sistema informático, o se excede en lo autorizado, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa.

Si el agente accede deliberada e ilegítimamente, en todo o en parte, al sistema informático vulnerando las medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa.

Será reprimido con la misma pena, el que accede a un sistema informático con el ánimo de apoderarse, divulgar o utilizar la información contenida en el sistema informático.

Artículo 4. Atentado a la integridad de sistemas informáticos

El que deliberada e ilegítimamente obstaculice o impida el normal funcionamiento, total o parcialmente, de un sistema informático, a través de la introducción, transmisión, daño, deterioro, alteración o supresión de datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa.

Disposición complementaria

Única. Reglamentación

El Poder Ejecutivo, en plazo máximo de sesenta (60) días calendarios, aprueba las normas reglamentarias que correspondan, conforme a lo dispuesto en la presente ley.

10.26.2. Exposición de motivos

Véase el texto completo de esta exposición de motivos en el siguiente enlace:	

10.26.3. Comentarios

Esta última propuesta legislativa recomienda modificar dos delitos que vulneran la seguridad informática y que han sido estudiados en esta obra:

a) Acceso ilícito: si bien mantiene la estructura actual, de forma escalonada propone sancionar (1) el acceso sin autorización o el exceso, sin vulneración de medidas de seguridad, (2) el acceso con ruptura o vulneración de medidas de seguridad y (3) el intrusismo malicioso, es decir, con un propósito ilícito adicional.

b) Ataques contra los sistemas informáticos: de forma adecuada sugiere reformular el tipo penal para alinearlo a la estructura legal sugerida en el Convenio de Budapest. No obstante, no incluye el elemento *gravedad* como ha sido recomendado en el citado instrumento internacional –y adoptado en la legislación comparada–.

EPÍLOGO

Pocos días antes de enviar a impresión este libro, se publicó el 29 de abril de 2025, la Ley N.º 32314, Ley que modifica el Código Penal, Decreto Legislativo 635, y la Ley 30096, Ley de delitos informáticos, para incluir el uso de la inteligencia artificial en la comisión de delitos. El artículo 2 de dicha norma modificó el artículo 11 de la Ley 30096, Ley de Delitos Informáticos, incorporando el numeral 5 en los siguientes términos:

> **Art. 11 LDI.- Agravantes**
>
> El juez aumenta la pena privativa de libertad hasta en un tercio por encima del máximo legal fijado para cualquiera de los delitos previstos en la presente Ley cuando:
>
> [...]
>
> 5. El agente comete el delito empleando la inteligencia artificial o tecnologías similares o análogas.

Esta norma tiene su origen en el Proyecto de Ley N.º 10525/2024, presentado el 14 de marzo del 2025, titulado *Ley que modifica los artículos 217, 218, 219, 220, 220-A, 220-B y 220-C del Decreto Legislativo N.º 635, Código Penal, a fin de optimizar la protección del derecho de propiedad intelectual ante los riesgos de la Inteligencia Artificial, y el artículo 402 a fin de optimizar la prevención de la violencia contra la mujer y los integrantes del grupo familiar y los delitos de corrupción de funcionarios.*

A dicho proyecto se acumuló el Proyecto N.º 6573/2023-CR, presentado el 4 de diciembre del 2023[897] por la congresista María del Carmen Alva, titu-

897 El Proyecto de Ley N.º 6573-2023-CR fue remitido a la Comisión de Justicia y Derechos Humanos del Congreso de la República el 5 de diciembre del 2023.

lado *Ley que incorpora como agravante la utilización de la Inteligencia Artificial para la comisión de delitos.* Esta fue la propuesta que sugirió incluir una quinta modalidad de circunstancias agravantes al artículo 11 LDI.

Si bien en la exposición de motivos no se desarrollaron las razones que justifican incluir esta circunstancia agravante a nuestra ley especial, el 14 de abril del 2025, la Comisión de Justicia y Derechos Humanos del Congreso emitió un dictamen en el que acumuló cuatro proyectos de ley: 6573/2023-CR, 7072/2023-CR, 8746/2024-CR y 10525/2024-CR. Así, el dictamen fue favorable y se recomendó aprobar los proyectos en referencia con un texto sustitutorio[898].

Finalmente, el 16 de abril se aprobó en primera votación y, además, se exoneró de la segunda votación, quedando lista para su promulgación por el Poder Ejecutivo, tal como finalmente ocurrió.

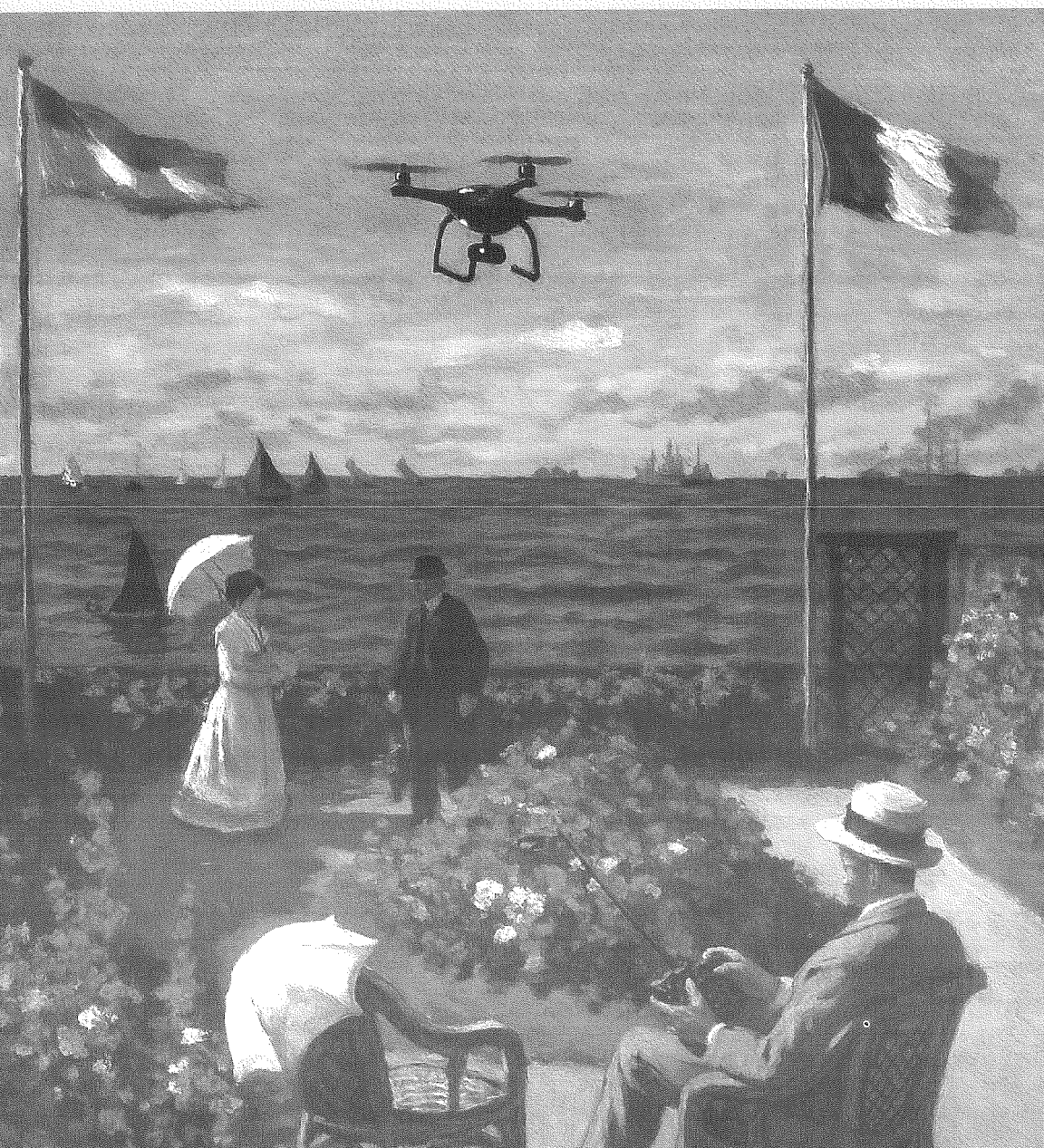
Esta obra no puede esperar el derrotero legislativo, pero sí advertir que el derecho penal está evolucionando para sancionar nuevas formas de criminalidad y responder a las herramientas que facilitan su comisión. De este modo, el lector debe empaparse tanto de información y conocimiento del derecho como de

898 Sobre la IA, en el análisis sobre la necesidad, viabilidad y oportunidad de la propuesta legislativa, se señala que "la Inteligencia Artificial (IA) es una herramienta tecnológica que permite crear programas capaces de aprender y decidir a semejanza de las funciones propias de la mente humana, en el que los principales desafíos que en la actualidad enfrenta esta tecnología, a nivel regulatorio, sin el incumplimiento de las leyes de protección de datos personales, la violación de derechos de propiedad intelectual, la discriminación, el acoso cibernético, entre otros; por lo que requiere con urgencia un marco normativo que sancione su mala implementación. La presente iniciativa legislativa propone (...) Modificar el artículo 11 de la Ley 30096, Ley de Delitos Informáticos". Más adelante, en el Análisis Costo Beneficio, se precisa que tendrá un impacto social positivo: "La propuesta legislativa beneficiará a la sociedad, puesto que, prioriza seguridad de los datos a ser utilizados por personas naturales, jurídicas e instituciones u organismos públicos y privados por medio de la tecnología, cuando se trate de utilización y procesamiento de cálculos o bases de datos en operaciones de ámbito público o público privado, estableciendo medios disuasivos respecto al mal uso de la inteligencia artificial, cuando se destina a la comisión de delitos de diversa índole, que afectan los derechos de las personas, combatiendo el uso inapropiado de la Inteligencia Artificial (IA) que pueda perjudicar a grupos vulnerables. Además, se busca proteger a millones de niños, adolescentes y población en general, toda vez que se disuadirá el mal uso de las tecnologías de inteligencia artificial, similares o análogas".

disciplinas nuevas para comprender este desarrollo y estar preparados para los cambios que nos depara el futuro.

Sea en una segunda edición o en un próximo texto, espero abordar la relación de la inteligencia artificial y el derecho penal. Esta labor no puede resumirse en pocas líneas, ya que exige hacerse en profundidad y con seriedad académica.

ANEXOS



* La ilustración de la página anterior corresponde a una adaptación de *La terraza de Sainte-Adresse* de Claude Monet (1867). Para su elaboración, se empleó OpenAI.

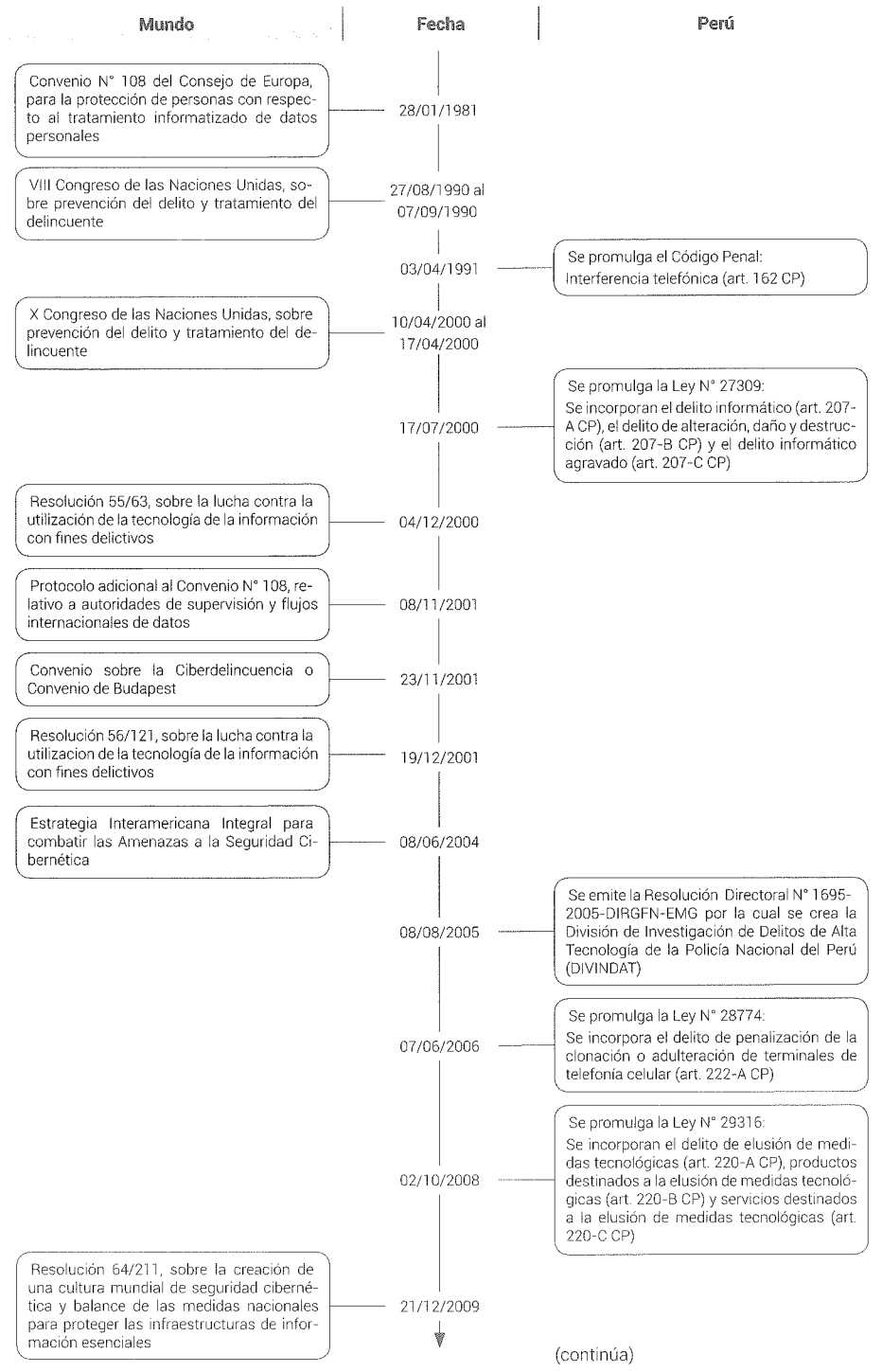
ANEXOS

Sumario: Anexo A. Línea de tiempo de los ciberdelitos contra la seguridad informática. **Anexo B.** Dictamen de la Comisión Ad Hoc de Justicia y Derechos Humanos, recaído en los Proyectos de Ley N.^{os} 034/2011-CR, 307/2011-CR y 1136/2011-CR. **Anexo C.** Diario de debates, 12 de setiembre de 2013. **Anexo D.** La enseñanza de la ciberdelincuencia en la educación superior.

ANEXO A. LÍNEA DE TIEMPO DE LOS CIBERDELITOS CONTRA LA SEGURIDAD INFORMÁTICA

A continuación, se presenta una línea de tiempo que recoge los eventos más importantes, a nivel legislativo y de política criminal, que guardan relación con los ciberdelitos, de forma general, y los ataques contra la seguridad informática, en particular. De este modo, quedan excluidos los ciberdelitos réplica y de contenido –es decir, los ilícitos que lesionan bienes jurídicos tradicionales como el patrimonio, la libertad e indemnidad sexual, la propiedad intelectual, entre otros–.

En la columna denominada "Mundo", se recogen los esfuerzos internacionales en la materia: sistemas de las Naciones Unidas, europeo e interamericano. En la columna "Fecha", se coloca el día o el periodo en el que se produjo el acontecimiento resaltado. Finalmente, en la columna "Perú", se presentan los eventos legislativos más relevantes, indicando su relación específica con los delitos estudiados en esta obra, así como la creación de los órganos especializados encargados de su persecución.


Mundo
Fecha
Perú
Convenio N° 108 del Consejo de Europa, para la protección de personas con respecto al tratamiento informatizado de datos personales
28/01/1981
VIII Congreso de las Naciones Unidas, sobre prevención del delito y tratamiento del delincuente
27/08/1990 al 07/09/1990
03/04/1991
Se promulga el Código Penal: Interferencia telefónica (art. 162 CP)
X Congreso de las Naciones Unidas, sobre prevención del delito y tratamiento del delincuente
10/04/2000 al 17/04/2000
17/07/2000
Se promulga la Ley N° 27309: Se incorporan el delito informático (art. 207-A CP), el delito de alteración, daño y destrucción (art. 207-B CP) y el delito informático agravado (art. 207-C CP)
Resolución 55/63, sobre la lucha contra la utilización de la tecnología de la información con fines delictivos
04/12/2000
Protocolo adicional al Convenio N° 108, relativo a autoridades de supervisión y flujos internacionales de datos
08/11/2001
Convenio sobre la Ciberdelincuencia o Convenio de Budapest
23/11/2001
Resolución 56/121, sobre la lucha contra la utilizacion de la tecnología de la información con fines delictivos
19/12/2001
Estrategia Interamericana Integral para combatir las Amenazas a la Seguridad Cibernética
08/06/2004
08/08/2005
Se emite la Resolución Directoral N° 1695-2005-DIRGFN-EMG por la cual se crea la División de Investigación de Delitos de Alta Tecnología de la Policía Nacional del Perú (DIVINDAT)
07/06/2006
Se promulga la Ley N° 28774: Se incorpora el delito de penalización de la clonación o adulteración de terminales de telefonía celular (art. 222-A CP)
02/10/2008
Se promulga la Ley N° 29316: Se incorporan el delito de elusión de medidas tecnológicas (art. 220-A CP), productos destinados a la elusión de medidas tecnológicas (art. 220-B CP) y servicios destinados a la elusión de medidas tecnológicas (art. 220-C CP)
Resolución 64/211, sobre la creación de una cultura mundial de seguridad cibernética y balance de las medidas nacionales para proteger las infraestructuras de información esenciales
21/12/2009

(continúa)

Mundo	Fecha	Perú
XII Congreso de las Naciones Unidas, sobre Estrategias amplias ante problemas globales	12/04/2010 al 19/04/2010	
Declaración de Río sobre el Delito Cibernético	23/03/2012	
	19/08/2013	**Se promulga la Ley N° 30076. Ley de delitos informáticos (LDI)** Se incorpora el delito de tráfico ilegal de datos (art. 207-D CP)
	22/10/2013	Se promulga la Ley N° 30096: Se incorporan el delito de acceso ilícito (art. 2 LDI), atentado contra datos y sistemas informáticos (arts. 3 y 4 LDI), interceptación ilícita (art. 7 LDI) y abuso de mecanismos y dispositivos informáticos (art. 10 LDI)
	10/03/2014	Se promulga la Ley N° 30171: Se modifican el delito de acceso ilícito (art. 2 LDI), atentado contra datos y sistemas informáticos (arts. 3 y 4 LDI), interceptación ilícita (art. 7 LDI) y abuso de mecanismos y dispositivos informáticos (art. 10 LDI)
Convenio Iberoamericano de Cooperación sobre investigación, aseguramiento y obtención de prueba en materia de ciberdelincuencia	28/05/2014	
XIII Congreso de las Naciones Unidas, sobre prevención del delito y tratamiento del delincuente	12/04/2015 al 19/04/2015	
Directiva 2016/680 del Parlamento Europeo y del Consejo de Europa	27/04/2016	
	01/12/2019	En el Perú, entra en vigor el Convenio sobre la Ciberdelincuencia o Convenio de Budapest.
Informe de la Reunión del Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético	27/07/2020 al 29/07/2020	
	30/12/2020	Se promulga la Resolución de la Fiscalía de la Nación N° 1503-2020-MP-FN por la cual se crea la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público.
	15/02/2021	La Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público empieza a ejercer funciones, con carga cero.
	15/06/2021	Se crea la Fiscalía Especializada en Ciberdelincuencia de Lima Centro.
XIV Congreso de las Naciones Unidas, sobre prevención del delito y justicia penal	07/03/2021 al 12/03/2021	
	26/09/2023	Se crea la Fiscalía Especializada en Ciberdelincuencia de La Libertad.
	13/10/2023	Se crea la Fiscalía Especializada en Ciberdelincuencia de Arequipa.
	20/12/2023	Se promulga el Decreto Legislativo N° 1614: Se modifica el delito de acceso ilícito (art. 2 LDI)

ANEXO B. DICTAMEN DE LA COMISIÓN AD HOC DE JUSTICIA Y DERECHOS HUMANOS, RECAÍDO EN LOS PROYECTOS DE LEY N.OS 034/2011-CR, 307/2011-CR Y 1136/2011-CR

Véase el texto completo de este anexo en el siguiente enlace:

ANEXO C. DIARIO DE DEBATES, 12 DE SETIEMBRE DEL 2013

Véase el texto completo de este anexo en el siguiente enlace:

ANEXO D. LA ENSEÑANZA DE LA CIBERDELINCUENCIA EN LA EDUCACIÓN SUPERIOR

Desde el 2022, la maestría de Derecho Penal de la Pontificia Universidad Católica del Perú me ha brindado la oportunidad de impartir el módulo *Ciber-criminalidad* que integra el curso *Derecho Penal y nuevas formas de criminalidad.* Así, desde nuestra universidad se vienen impulsando diversas tesis tanto en pregrado como en posgrado que evidencian la importancia de esta disciplina, así como del tratamiento de la prueba digital.

D.1. Propuesta pedagógica

Lamentablemente, a nivel de estudios de pregrado, esto es, en las facultades de derecho de América Latina, son muy pocas las universidades que han incluido este curso como parte de la malla curricular. Por esta razón, en estas breves líneas, compartiré una propuesta pedagógica que he diseñado y que,

quizás, sea de utilidad para otros docentes o gestores curriculares que deseen incorporar el curso denominado *Delitos informáticos y cibercriminalidad*[899].

1. Título del curso

   Delitos informáticos y cibercriminalidad

2. Fundamentación o justificación del curso

   La evolución de la ciberdelincuencia ha obligado a los sistemas jurídicos de diversos países a actualizar sus normativas para enfrentar nuevas amenazas en el entorno digital. A lo largo de los años, muchas jurisdicciones han tipificado los delitos informáticos, reconociendo la necesidad de contar con legislaciones especializadas y unidades de investigación dedicadas a su persecución.

   Sin embargo, el avance tecnológico ha permitido el surgimiento de nuevas modalidades delictivas, como el sabotaje informático, el fraude digital, la suplantación de identidad, el lavado de criptoactivos y el *grooming*, entre otros. Estas conductas no solo afectan a individuos y empresas, sino que representan un desafío transnacional, pues los ciberdelincuentes pueden operar desde cualquier parte del mundo sin necesidad de estar físicamente en el país donde cometen el delito.

   Ante este panorama, la cooperación internacional ha cobrado gran relevancia. Organismos y tratados como el Convenio de Budapest sobre Ciberdelincuencia y la Convención de las Naciones Unidas contra la Ciberdelincuencia han servido como marco para armonizar legislaciones, fortalecer la colaboración entre Estados y mejorar las capacidades de investigación de los cuerpos policiales y fiscales. Asimismo, la creación de unidades especializadas en ciber-

899 Agradezco a mis diferentes profesores de la maestría de *Docencia Universitaria* cursada en la Pontificia Universidad Católica del Perú, ya que los elementos del sílabo que se describirán, su justificación y el material de enseñanza fue ideado, presentado y evaluado en las diferentes asignaturas cursadas. Además, expreso mi gratitud al Departamento de Ciencias Sociales y Humanas de la Universidad Católica Boliviana San Pablo, por haberme invitado a dictar el curso *Inteligencia artificial, ciberseguridad y ciberdelito*. Esta experiencia me ha permitido ejecutar la propuesta académica que se aborda en esta sección.

delincuencia ha sido clave para combatir estos delitos de manera más efectiva.

En un mundo cada vez más interconectado, comprender la ciberdelincuencia desde una perspectiva global es esencial. No basta con que cada país establezca sanciones; es fundamental contar con estrategias coordinadas, marcos normativos adaptables y cooperación internacional para enfrentar el cibercrimen, un fenómeno que no conoce fronteras.

Todos estos avances son un desafío constante contra la criminalidad organizada, quienes, con el apoyo del desarrollo tecnológico de su lado, han sofisticado su quehacer delictivo y con ello es un reto constante a las legislaciones modernas y muchas veces precarias como las nuestras.

En este escenario, este curso se orienta a la identificación y análisis de diversos delitos comprendidos en tres unidades académicas: (1) Ciberdelitos contra la seguridad informática, (2) Ciberdelitos contra el patrimonio y (3) Ciberdelitos contra la libertad e indemnidad sexual.

Este curso le permitirá al estudiante alcanzar competencias específicas: (1) Marco ético de la profesión: El análisis de declaraciones policiales y fiscales, así como resoluciones judiciales, permitirá que el estudiante comprenda la necesidad de una formación interdisciplinaria y especializada. (2) Exigencia académica: El estudiante conocerá normas especializadas como legislación comparada, el Convenio de Budapest y su Informe Explicativo, la Convención de las Naciones Unidas contra la Ciberdelincuencia, así como doctrina y jurisprudencia actual en la materia. (3) Relación con el entorno profesional: El estudiante conocerá cómo se investiga la ciberdelincuencia y los principales actores que participan en su persecución y juzgamiento. (4) Paradigma del Estado Constitucional de Derecho: El estudiante reconocerá nuevos bienes jurídicos de relevancia constitucional que se encuentran protegidos en la legislación local y comparada como la seguridad informática -compuesta por la integridad, confidencialidad y disponibilidad

de datos y sistemas informáticos-, el patrimonio, la libertad e indemnidad sexual, entre otros.

3. Justificación del curso[900]

Competencia	Resultado de aprendizaje
1. **Marco ético de la profesión:** Analiza la actuación de los operadores jurídicos, de manera ética y crítica, para contribuir con el desarrollo eficaz de los procesos.	1. Reconoce los aciertos y errores cometidos por la policía y la fiscalía en el marco de una investigación de ciber-criminalidad. 2. Comprende la importancia de la entrevista policial y fiscal al recibir la declaración de una víctima de ciberdelincuencia.
2. **Excelencia académica:** Incorpora conocimientos jurídicos actuales y adecuados para resolver consultas y controversias, priorizando el respeto de los derechos fundamentales.	3. Diferencia los ciberdelitos contra la seguridad informática, patrimonial e indemnidad y libertad sexual en la resolución de casos. 4. Redacta un documento jurídico, tomando en cuenta los hechos, los ciberdelitos y las pruebas necesarias.
3. **Relación con el entorno profesional:** Diferencia la estructura y el funcionamiento de las organizaciones nacionales e internacionales, en el ámbito de su especialidad, para propiciar una asesoría adecuada.	5. Diferencia las funciones de la policía y de la fiscalía en el marco de una investigación cibercriminal. 6. Reconoce las leyes nacionales e internacionales que sancionan la ciberdelincuencia atendiendo a los hechos denunciados.
4. **Paradigma del Estado Constitucional de Derecho:** Reconoce y utiliza los principios del Estado Constitucional de Derecho y los derechos fundamentales, con una actitud reflexiva y coherente, para tutelar los bienes jurídicos.	7. Identifica el bien jurídico protegido según el tipo de ciberdelito investigado. 8. Analiza los retos de la investigación de la ciberdelincuencia según la complejidad de los hechos.

4. Contenido del aprendizaje

El curso comprende tres unidades.

La primera ubica al estudiante frente al contexto nacional e internacional de la ciberdelincuencia y, en particular, de los delitos puros que atentan contra la integridad, disponibilidad y confidencialidad -elementos que componen la seguridad informática-. Se centra en el análisis del acceso ilícito, atentados contra los datos y sistemas informáticos, así como en el abuso de mecanismos informáticos y la interceptación ilícita.

La segunda unidad aborda los ciberdelitos más frecuentes, conocidos como delitos réplica, pues utilizan las Nuevas Tecnologías para facilitar su comisión. De este modo, el estudiante analizará las estafas en entornos virtuales, los fraudes informáticos, el lavado de criptoactivos y la ciberdelincuencia organizada.

900 He tomado como modelo el perfil del egresado de la Facultad de Derecho PUCP para identificar las competencias específicas del curso.

Finalmente, en la tercera unidad, el estudiante conocerá las principales manifestaciones de la ciberdelincuencia que atenta contra la libertad e indemnidad sexual, representado por el grooming, la pornografía infantil, la violencia de género en línea y la cibercriminalidad organizada relacionada a la captación de niños, niñas y adolescentes a través de medios digitales.

UNIDAD 1: CIBERDELITOS CONTRA LA SEGURIDAD INFORMÁTICA

Contenidos conceptuales	Contenidos procedimentales	Contenidos actitudinales
1.1 Introducción a la ciberdelincuencia 1.2 Marco normativo nacional e internacional relacionado a la ciberdelincuencia 1.3 Acceso ilícito 1.4 Atentado contra los datos y sistemas informáticos 1.5 Abuso de mecanismos informáticos e interceptación ilícita	• Comparación de cinco ciberdelitos contra la seguridad informática. • Análisis de los elementos objetivos y subjetivos de cada ciberdelito contra la seguridad informática. • Diseño de un plan para la investigación de ciberdelitos contra la seguridad informática. • Elaboración de un informe jurídico sobre ciberdelitos que atentan contra la seguridad informática.	• Reflexiona sobre la evolución legislativa de los ciberdelitos contra la seguridad informática. • Usa normas locales e internacionales sobre ciberdelitos contra la seguridad informática. • Opina críticamente sobre los ciberdelitos contra la seguridad informática.

UNIDAD 2: CIBERDELITOS CONTRA EL PATRIMONIO

Contenidos conceptuales	Contenidos procedimentales	Contenidos actitudinales
2.1 Estafa en entornos virtuales 2.2 Fraude informático 2.3 Ciber-lavado de activos 2.4 Cibercriminalidad organizada patrimonial	• Comparación de la estafa virtual con el fraude informático. • Análisis de las nuevas formas de lavado de activos, a través de criptoactivos. • Identificación de las características de una ciber organización criminal orientada a cometer delitos contra el patrimonio. • Diseño de un plan para la investigación de ciberdelitos contra el patrimonio. • Participación en una entrevista a una víctima de ciberdelito patrimonial.	• Usa normas locales referidas a ciberdelitos patrimoniales. • Reflexiona sobre el aumento exponencial de ciberdelitos patrimoniales. • Opina críticamente sobre el uso de los criptoactivos. • Escucha activamente a posibles víctimas de ciberdelito patrimonial.

UNIDAD 3: CIBERDELITOS CONTRA LA LIBERTAD E INDEMNIDAD SEXUAL

Contenidos conceptuales	Contenidos procedimentales	Contenidos actitudinales
3.1 Grooming o proposiciones sexuales a niños, niñas y adolescentes 3.2 Distribución de imágenes o videos de abuso sexual infantil 3.3 Violencia de género en línea 3.4 Cibercriminalidad organizada vinculada a la trata de personas	• Comparación de ciberdelitos contra la libertad e indemnidad sexual. • Comparación de ciberdelitos de violencia de género. • Análisis de diferentes modelos de captación, a través de entornos digitales. • Diseño de un plan para la investigación de ciberdelitos contra el la libertad e indemnidad sexual. • Elaboración de una denuncia por ciberdelitos contra la libertad e indemnidad sexual.	• Usa normas locales referidas a ciberdelitos contra la libertad e indemnidad sexual. • Reflexiona sobre el control de los entornos digitales de los menores de edad. • Reflexiona sobre el rol de los docentes y directores en la detección de violencia de género en línea y de posibles víctimas contra la libertad e indemnidad sexual. • Se compromete éticamente en la elaboración de una denuncia que involucre menores de edad.

5. Estrategias didácticas o metodología

La estrategia didáctica del curso responde a un modelo de corte constructivista que incentiva la participación de los estudiantes, tomando como base sus conocimientos previos, obtenidos en cursos, experiencias propias o en las prácticas preprofesionales. El rol del docente será de facilitador de información, pues si bien realizará algunas exposiciones al inicio de clase, incentivará la participación y reflexión de los alumnos. De este modo, se espera que los estudiantes sean responsables y revisen anticipadamente el material seleccionado.

En este sentido, siguiendo la colección "Métodos de formación jurídica" de la Facultad de Derecho PUCP, se aplican las siguientes estrategias de enseñanzas:

a. **Clase magistral activa:** Esta estrategia de enseñanza es una exposición dialogada en la que el docente interactúa con los estudiantes, promoviendo su participación. Por esta razón, cada semana se le pedirá al estudiante que revise un video, una noticia o una lectura que incentive el diálogo y la discusión.

b. **Estudio de casos:** Esta técnica activa permitirá que el estudiante aborde un caso diseñado por el docente. En el curso, se planteará un caso que será resuelto de forma grupal y que les

permitirá interactuar con entornos digitales ya que deberán buscar "las pruebas" en diferentes redes sociales.

c. **Aprendizaje basado en problemas:** Esta técnica activa permite que los estudiantes reflexionen, investiguen y discutan a partir de situaciones problemáticas propuestas por el docente que, en el curso, se traducen en noticias actuales vinculadas a la cibercriminalidad.

d. **Trabajo colaborativo:** Esta técnica activa permitirá que los estudiantes realicen un trabajo colaborativo que se presentará al final del curso y que consistirá en un trabajo de investigación jurídico.

e. **Debate:** Esta técnica de enseñanza-aprendizaje permitirá que los estudiantes confronten sus posiciones respecto a problemas jurídicos como el uso de la inteligencia artificial o la regulación de las nuevas tecnologías.

Los principales medios y materiales educativos que se emplearán son: (1) casos diseñados por el docente, (2) noticias de actualidad que involucren cibercrímenes, (3) disposiciones de archivo o resoluciones judiciales emblemáticas vinculados a la cibercriminalidad, (4) extractos de películas y series relacionadas a los ciberdelitos y su investigación. Es importante precisar que se contará con (5) sesiones virtuales con tres profesores extranjeros, de diferentes disciplinas, que enriquecerán la discusión jurídica.

Toda vez que cada facultad establece el número de clases, carga lectiva, semanas de duración y sistemas de evaluación, he preferido no desarrollar estos tópicos y, de este modo, evitar confusiones.

D.2. Material de enseñanza

La enseñanza de la cibercriminalidad y su investigación es una labor compleja. Por esta razón, el profesor **Vladimir Padilla Alegre** y el autor de esta obra, diseñamos los ejercicios que, a continuación, se detallan y que fueron empleados, por primera vez, en el curso Derecho Procesal Penal Especial,

dictado en la Facultad de Derecho de la Pontificia Universidad Católica del Perú (2025-1)[901].

Se autoriza el uso, la adaptación y la reproducción de los ejercicios diseñados, pero los autores debemos ser citados.

D.2.1. Veinte ejercicios sobre ciberdelincuencia

Los ejercicios que se describen a continuación, pueden ser empleados por los docentes con las siguientes finalidades:

- Analizar la modalidad delictiva y compararla con los casos que se suscitan en el ámbito local o realidad nacional.
- Ejercitar el juicio de subsunción a la legislación penal local o compararla con la regulación propuesta en el Convenio de Budapest o la Convención de las Naciones Unidas contra la Ciberdelincuencia.
- Proponer hipótesis de investigación, a partir del caso analizado.
- Proponer actos de investigación, tomando como base el caso evaluado.

1. Ejercicio 1. El *ransomware* en el hospital público

En una ciudad pequeña de América Latina, el Hospital General de San Marcos sufrió un ciberataque que paralizó sus sistemas en plena emergencia por un brote de dengue. El atacante, que utilizó un *ransomware* llamado "Medilock", encriptó las historias clínicas, los registros de pacientes y el acceso a los equipos de diagnóstico. El hospital recibió un mensaje exigiendo 50 bitcoins para desbloquear la información, amenazando con filtrar datos sensibles de los pacientes y de los médicos.

El director del hospital, Dr. Juan Paredes, enfrentó la difícil decisión de pagar el rescate o denunciar el ataque, ya que la falta de acceso a los sistemas ponía en riesgo vidas humanas. Sin embargo, tras consultar con expertos legales y en ciberseguridad, optaron por involucrar a la policía cibernética del

901 En la elaboración de los casos, se hizo uso de distintas herramientas de Inteligencia Artificial, atendiendo a los significativos beneficios que ofrecen para la enseñanza.

país. Durante la investigación, descubrieron que el ataque provenía de una red internacional con servidores ubicados en Europa del Este.

2. Ejercicio 2. La empresa de *software* en Silicon Valley.

"SoftDev Solutions", una prometedora empresa tecnológica ubicada en Silicon Valley, sufrió un ataque de *ransomware* que detuvo la operación de su plataforma de desarrollo colaborativo. El atacante, identificado como "ShadowByte", utilizó ingeniería social para acceder al sistema de un empleado clave, engañándolo con un correo que simulaba ser de un cliente.

Una vez dentro, el atacante desplegó un *ransomware* que cifró toda la infraestructura de desarrollo y las bases de datos de clientes. Exigieron 1 millón de dólares en criptomonedas y amenazaron con divulgar el código fuente de la empresa en la *dark web*. El CEO, Lisa Chen, contrató de inmediato a una firma de ciberseguridad y descubrieron que parte de la responsabilidad recaía en un contrato externo con un proveedor que no cumplía estándares mínimos de seguridad.

3. Ejercicio 3. La universidad hackeada en Europa

La Universidad de Oxford fue atacada por un grupo conocido como "CryptoScholars". Este *ransomware* atacó principalmente la base de datos del departamento de investigaciones biomédicas, encriptando avances relacionados con un tratamiento experimental contra el cáncer.

El mensaje de los atacantes indicaba que liberarían la información si pagaba un rescate de 200.000 euros en Monero, una criptomoneda de difícil rastreo. La universidad, preocupada no solo por la pérdida de la información, sino también por el daño reputacional, enfrentó presiones del gobierno británico y de las empresas farmacéuticas asociadas para no negociar con los ciberdelincuentes.

4. Ejercicio 4. El despacho de abogados víctima de *ransomware*

Un prestigioso despacho de abogados en Nueva York, "Silverman & Partners", especializado en litigios corporativos, fue víctima de un *ransomware* durante un importante caso de arbitraje internacional. Los atacantes, un grupo denominado "LawFang", lograron acceso mediante un enlace malicioso enviado al socio más joven del despacho.

El *ransomware* cifró documentos confidenciales relacionados con el arbitraje y exigió un rescate de 500.000 dólares para desbloquearlos. Ante el dilema de proteger la privacidad de los clientes y el impacto en su reputación, los socios debatieron si pagar o buscar ayuda externa. De este modo, la discusión se centró si el apoyo debía ser oficial o si podían contratar a personal técnico (terceros).

5. Ejercicio 5. El *ransomware* en una PYME

"Delicias Doña Clara", una pyme de repostería artesanal en México, fue víctima de un ataque de *ransomware* que paralizó su sistema de ventas en línea justo antes de Navidad, su temporada más lucrativa. El atacante, identificado como un hacker aficionado, envió un correo con un enlace malicioso bajo el pretexto de una oferta de software gratuito.

Aunque el rescate era relativamente bajo (10.000 pesos mexicanos), la dueña, Clara Ramírez, no sabía cómo proceder. Sin experiencia en ciberseguridad, optó por contratar a un experto local, quien descubrió que el atacante era un adolescente de su localidad

6. Ejercicio 6. El fraude del empresario argentino en la red social de inversiones

Carlos Fernández, un empresario de Buenos Aires, se registró en una red social exclusiva para inversores llamada "TradeNet". Allí publicó un perfil falso como un exitoso gestor de inversiones, mostrando supuestas ganancias de clientes y ofreciendo rendimientos garantizados de hasta un 25% mensual.

Carlos convenció a varios usuarios de transferir dinero a una cuenta bancaria a nombre de su empresa "Innova Capital". Utilizó los fondos de los nuevos inversionistas para pagar pequeños retornos a los primeros, simulando una operación legítima. Después de recaudar más de 2 millones de dólares, Carlos desapareció, dejando a decenas de víctimas con pérdidas económicas significativas.

7. Ejercicio 7. El *phishing* bancario en una pequeña ciudad española

Marta Gutiérrez, una empleada de una tienda en Toledo, recibió un correo aparentemente enviado por su banco. El mensaje indicaba que su cuenta sería suspendida si no confirmaba sus datos. Presionada por la urgencia, Marta

ingresó al enlace del correo y completó un formulario con su información personal y bancaria.

Dos días después, Marta descubrió que habían transferido 3.000 euros de su cuenta a una dirección desconocida. La investigación reveló que el enlace dirigía a una página web clonada del banco, administrada por un grupo de ciberdelincuentes en Europa del Este.

8. Ejercicio 8. La estafa en la criptomoneda en Dubái

Ahmed Al-Mansoor, un joven emprendedor en Dubái, lanzó un supuesto proyecto de criptomoneda llamado "GoldenCoin". Prometía ser la próxima gran revolución en el mercado digital, con una oferta inicial de monedas (ICO) diseñada para recaudar fondos de inversionistas globales.

Ahmed utilizó redes sociales y conferencias virtuales para atraer a miles de inversionistas, quienes compraron "GoldenCoin" por un total de 15 millones de dólares. Poco después de recaudar el dinero, Ahmed cerró el sitio web del proyecto y transfirió los fondos a cuentas en paraísos fiscales. Las autoridades descubrieron que no había ningún desarrollo tecnológico detrás del proyecto, solo una fachada bien diseñada.

9. Ejercicio 9. La suplantación de identidad en una tienda de lujo en New York

Samantha Jones, una ejecutiva en Manhattan, descubrió que alguien había utilizado su identidad para realizar compras por 20 000 dólares en una tienda de lujo. La investigación reveló que un ciberdelincuente había hackeado su correo electrónico, accediendo a documentos que contenían copias de su identificación y tarjeta de crédito.

El delincuente creó una cuenta falsa en la tienda, enviando los productos a una dirección temporal. Aunque Samantha denunció el caso y logró detener algunos cargos contra ella, el fraude afectó su calificación crediticia y le tomó meses resolver su situación.

10. Ejercicio 10. El fraude del empleo remoto en Filipinas

Jasmine Reyes, una madre soltera en Manila, encontró un anuncio en redes sociales para trabajar desde casa como asistente virtual. Tras ser contactada por "Global Remote Solutions", un supuesto empleador extranjero, Jasmine

recibió instrucciones para comprar equipos de trabajo (portátil y software), enviando un pago inicial como "garantía" a una cuenta bancaria.

Después de transferir 500 dólares, Jasmine perdió contacto con la empresa y se dio cuenta de que el anuncio era falso. Otros afectados también denunciaron el caso, pero no se pudo ubicar a todas las víctimas del fraude, porque los agraviados residían en diferentes partes del mundo.

11. Ejercicio 11. El *youtuber*

Tomás, un *youtuber* de 25 años con 500.000 suscriptores, crea contenido relacionado con videojuegos y tutoriales tecnológicos. A través de su popularidad, Tomás contacta a Lucía, una niña de 12 años, quien solía comentar sus videos. Comienza a conversar con ella en un tono amigable, hasta que, tras semanas de interacción, las conversaciones derivan en un contenido más personal y explícito.

Tomás convence a Lucía de enviarle fotografías íntimas bajo el pretexto de que "él la ayudaría a ser famosa en YouTube". La madre de Lucía encuentra las conversaciones y las imágenes en el teléfono de la niña, tras notar que se comportaba de forma extraña y retraída.

Tras una denuncia, la policía incauta los dispositivos de Tomás y descubre que ha contactado a otras niñas bajo el mismo esquema, acumulando una cantidad significativa de imágenes ilícitas.

12. Ejercicio 12. El videojuego en línea

Marco, un hombre de 35 años, utilizaba un popular videojuego en línea para contactar a menores de edad. Se hacía pasar por un jugador adolescente y comenzaba conversaciones con los menores a través del chat del juego. Con el tiempo, Marco ganó la confianza de Diego, un niño de 11 años, quien veía en él a un amigo.

Después de meses de interacción, Marco convenció a Diego de que le enviara fotos personales, bajo la promesa de regalarle equipamiento dentro del juego. Cuando los padres de Diego descubrieron las conversaciones y las imágenes, denunciaron el caso a la policía, que logró rastrear la dirección IP de Marco y detenerlo.

13. Ejercicio 13. La red social de moda y el perfil falso

Claudia, una niña de 13 años, comenzó a interactuar en una red social de moda donde compartía sus intereses por la fotografía. Recibió un mensaje de "Daniel", quien decía ser un fotógrafo profesional de 16 años. En realidad, "Daniel" era Rodrigo, un hombre de 38 años que creaba perfiles falsos para contactar a menores.

Rodrigo le ofreció a Claudia participar en un supuesto concurso fotográfico. A cambio, le pidió que enviara fotos en trajes específicos. Después de que Claudia compartió las imágenes, Rodrigo comenzó a pedir contenido más explícito, amenazando con publicar las fotos iniciales si no cumplía. Los padres de Claudia intervinieron cuando ella confesó lo ocurrido, y las autoridades detuvieron a Rodrigo tras rastrear el perfil falso.

14. Ejercicio 14. El maestro de informática y el abuso de confianza

Gustavo, un maestro de informática en una escuela primaria, utilizó su posición para acercarse a Sofía, una estudiante de 12 años. Bajo el pretexto de ayudarla con proyectos escolares, Gustavo comenzó a enviarle mensajes a través de aplicaciones de mensajería.

Al principio, los mensajes eran sobre tareas, pero poco a poco se tornaron más personales. Gustavo le pidió a Sofía que le enviara fotografías para "probar una aplicación educativa". Cuando la madre de Sofía revisó su teléfono, encontró las imágenes y denunció el caso a las autoridades escolares y policiales. Al investigar, descubrieron que Gustavo había realizado esto con varias niñas del colegio.

15. Ejercicio 15. El fotógrafo de la red social

Camila, una adolescente de 14 años apasionada por la moda y la fotografía, comenzó a compartir sus imágenes en una red social popular entre jóvenes. Allí fue contactada por "Andrés", un supuesto fotógrafo profesional que afirmaba trabajar para una revista de moda internacional. Andrés, cuyo verdadero nombre era Jorge Martínez, un hombre de 37 años, inició una conversación con Camila mostrándose amable y alentador, ganándose su confianza con halagos sobre su apariencia y talento.

Después de varias semanas de interacción, Jorge convenció a Camila de que tenía potencial para ser modelo y le ofreció participar en un casting virtual para una campaña internacional. Le pidió que enviara fotografías específicas en ropa ajustada para "evaluar su perfil físico". Camila, emocionada por la oportunidad, accedió y compartió las imágenes a través de la plataforma.

Al recibir las fotos, Jorge le pidió imágenes más comprometedoras, argumentando que eran requisitos para mostrar "versatilidad" en el modelaje. Cuando Camila dudó, Jorge la amenazó, diciendo que, si no cumplía, divulgaría las fotos que ya tenía a sus contactos y a la escuela donde estudiaba. Atormentada, Camila le contó lo sucedido a su hermana mayor, quien alertó a sus padres.

La familia denunció el caso a la policía, que identificó a Jorge como un depredador en línea con múltiples víctimas adolescentes en la región. La investigación reveló que Jorge utilizaba su perfil falso para contactar a menores en varias redes sociales y había almacenado una gran cantidad de material ilícito en sus dispositivos electrónicos.

16. Ejercicio 16. El perfil falso del director de empresa

Mariana Pérez, una joven emprendedora, recibió un mensaje en LinkedIn de "Eduardo Gutiérrez", quien se presentaba como director de una importante empresa tecnológica. Eduardo le ofreció participar en un proyecto innovador y le pidió detalles confidenciales sobre su modelo de negocio.

Mariana, emocionada por la oportunidad, compartió sus ideas y documentos confidenciales, incluyendo una copia de su plan de negocios. Semanas después, descubrió que "Eduardo" no existía y que su idea había sido registrada por otra empresa. La policía rastreó el perfil falso hasta Javier Ortega, un competidor que había creado la cuenta para robar información confidencial.

17. Ejercicio 17: El robo de identidad para préstamos bancarios

Carlos López, un empleado bancario, recibió notificaciones de préstamos a su nombre en varias entidades financieras. Al revisar su historial, descubrió que alguien había utilizado sus datos personales, incluidos su DNI y una copia falsificada de su firma, para solicitar créditos.

La investigación reveló que María Ríos, una antigua compañera de trabajo de Carlos, había accedido a su información personal mientras trabajaban juntos

y la había utilizado para cometer el fraude. Aunque María desapareció tras recibir los fondos, fue rastreada cuando intentó repetir el esquema en otra entidad.

18. Ejercicio 18: El impostor en redes sociales

Clara Sánchez, una *influencer* con más de 300.000 seguidores en Instagram, descubrió que alguien había creado una cuenta con su nombre y fotografías. El perfil falso contactaba a sus seguidores, solicitando transferencias bancarias con la excusa de recaudar fondos para una causa benéfica.

Cuando una seguidora intentó confirmar la campaña, Clara negó estar involucrada. Tras la denuncia, las autoridades identificaron a Antonio Ruiz, un hombre de 32 años, como el creador del perfil falso. Antonio utilizó las donaciones para financiar gastos personales.

19. Ejercicio 19: El impostor en redes sociales

Camilo Ramírez, un exempleado de la empresa "TechCorp", fue despedido por mal desempeño. En represalia, Camilo creó un correo electrónico falso con el nombre del gerente general de la empresa y envió mensajes a los clientes clave, informando que la empresa estaba en quiebra.

El daño fue inmediato: varios clientes cancelaron contratos, afectando gravemente la reputación de "TechCorp". Al ser denunciado, las autoridades rastrearon el correo hasta Camilo, quien fue acusado de suplantación y daño reputacional.

20. Ejercicio 20: La suplantación en una aplicación de citas

Martín, un joven de 28 años, fue contactado en una aplicación de citas por "Laura", una mujer que decía tener intereses similares. Tras semanas de conversaciones, "Laura" le pidió a Martín que compartiera fotos y datos personales para conocerse mejor.

Sin embargo, "Laura" era en realidad Francisco, un hombre de 40 años que utilizó las fotos y los datos de Martín para abrir cuentas bancarias y realizar compras en línea. Martín descubrió el fraude cuando recibió facturas por productos que nunca había comprado. La policía identificó a Francisco tras rastrear las cuentas falsas y los envíos de productos.

D.2.2. Ejercicio "El Abismo de la Confianza"

Este es un caso mucho más complejo que los veinte ejercicios que hemos desarrollado previamente. Exige que el estudiante esté familiarizado con los delitos informáticos y, además, conozca su legislación penal y procesal penal. El docente puede emplear el caso con las siguientes finalidades:

- Reflexionar sobre la implicancia ética de la develación de información privilegiada en un estudio de abogados.
- Discutir sobre las medidas de seguridad empleadas a nivel personal y profesional.
- Evaluar a los estudiantes y conocer si analizan adecuadamente los tipos penales estudiados.
- Elaborar una denuncia especializada en delitos informáticos, tomando como insumos los hechos descritos y los actos de investigación "particulares".
- Analizar el testimonio de los diferentes personajes y contrastarlo con el informe técnico de incidencia.
- Planificar las preguntas que formularía un fiscal a cada uno de los trabajadores y clientes de la firma de abogados.
- Diseñar un plan de investigación, desde la posición de la fiscalía.

1. Descripción general del caso y personajes.

El Estudio Jurídico "García & Asociados", una prestigiosa firma ubicada en San Isidro, Lima, enfrenta una serie de incidentes que ponen en riesgo su reputación, la privacidad de sus clientes y la integridad de su personal. Los hechos ocurren entre el 1 y el 15 de octubre de 2023, y se detectan varios incidentes dentro de la organización.

1.1. Luis García López: Socio fundador y dueño del estudio.

1.2. María Ortega Pérez: Abogada sénior, encargada del área penal.

1.3. Jorge Martínez Ramírez: Abogado corporativo.

1.4. Daniela Torres Rivas: Practicante de segundo año.

1.5. Carlos Hernández Vega: Practicante recién ingresado.

1.6. Raúl Jiménez Cruz: Jefe de Tecnología de la Información.

1.7. Beatriz Sánchez Flores: Jefa de Recursos Humanos.

1.8. Marta López Núñez: Secretaria de la recepción.

1.9. Sofía Morales Díaz: Cliente involucrada en un caso de divorcio.

1.10. Fernando Álvarez Soto: Cliente corporativo con un contrato confidencial.

2. Hechos

2.1. Luis García descubre que alguien ingresó sin autorización a su cuenta personal de una red social (Facebook), accediendo a conversaciones privadas con un socio de la firma contraria, "Rodríguez Abogados". En estas conversaciones se acuerdan estrategias que van en contra de los intereses de sus clientes. Las conversaciones fueron filtradas a medios digitales, dañando la reputación de ambas firmas.

2.2. Beatriz Sánchez, en colaboración con Raúl Jiménez, instala software espía en las computadoras de los abogados y practicantes. El objetivo era monitorear conversaciones y tareas laborales, justificándolo como una medida para "mejorar la productividad". Este software recolecta datos sin el consentimiento del personal.

2.3. Carlos Hernández, practicante, abre un correo con un archivo malicioso mientras juega en línea desde su celular. Este archivo infecta su computadora y, al estar conectada a la red del estudio, permite al atacante acceder a información confidencial del servidor. El atacante cifra los datos del servidor y exige un rescate de 3 bitcoins para no divulgar la información.

3. Testimonio de Luis García López, socio fundador

Fecha: 20 de octubre de 2023.

Lugar: Sala de juntas del Estudio Jurídico García & Asociados.

El día 5 de octubre de 2023, aproximadamente a las 8:30 de la mañana, me encontraba en mi oficina revisando correos electrónicos cuando recibí una llamada de un periodista de un medio digital conocido. Me informaron que habían recibido capturas de pantalla de conversaciones privadas de mi cuenta personal de Facebook. Estas conversaciones, de carácter extremadamente confidencial, se llevaron

a cabo con Alejandro Rodríguez, socio principal de 'Rodríguez Abogados'. En ellas discutíamos términos que podríamos llamar antitéticos a nuestra ética profesional, relacionados con un acuerdo en el caso 'Inmobiliaria Tres Torres S.A.' Al principio, pensé que se trataba de una extorsión, pero poco después me percaté de que mi cuenta había sido vulnerada. Revisé el registro de actividad en mi perfil y noté que el 3 de octubre a las 11:47 p.m. hubo un acceso desde una dirección IP desconocida en Tijuana, Baja California. Este acceso no fui yo quien lo realizó. Intenté cambiar mi contraseña, pero para entonces las conversaciones ya estaban publicadas en foros legales y páginas de noticias.

Esto ha generado un daño inmenso a la firma y, por supuesto, a mi reputación. Exijo una investigación profunda, ya que esto no solo compromete nuestra credibilidad, sino que puede derivar en sanciones graves tanto para mi persona como para el bufete.

4. Testimonio de María Ortega Pérez, abogada *senior*

Fecha: 21 de octubre de 2023.

Lugar: Sala de juntas del Estudio Jurídico García & Asociados.

El 6 de octubre de 2023, fui convocada por el licenciado Luis García a su despacho para analizar el impacto de la filtración de las conversaciones privadas que habían sido publicadas en diversos medios. Él estaba visiblemente alterado y nos pidió a mí y a Jorge Martínez que revisáramos si los casos en curso podían verse afectados. Esa mañana, al intentar acceder a algunos de mis archivos relacionados con el caso 'Inmobiliaria Tres Torres S.A.', noté que mis documentos estaban duplicados en una carpeta que yo no había creado.

También recordé que, desde la semana anterior, el 3 de octubre, mi computadora había presentado comportamientos extraños. Por ejemplo, ventanas que se abrían solas y accesos a mis correos en horarios en los que no estaba trabajando. Informé de esto al área de TI, pero Raúl Jiménez me aseguró que era 'un problema de actualizaciones'.

Considero que estos eventos están relacionados con el acceso no autorizado que ocurrió en la red de la firma. Esto afecta gravemente nuestro trabajo y la confianza de los clientes.

5. Testimonio de Jorge Martínez Ramírez, abogado corporativo

Fecha: 22 de octubre de 2023.

Lugar: Oficina privada de Jorge Martínez.

El 5 de octubre de 2023, recibí una llamada de Sofía Morales, una de nuestras clientas, quien me preguntó si su caso de divorcio se encontraba seguro. Me sorprendió su pregunta, pero no pude darle una respuesta concreta porque, minutos antes, había escuchado en los pasillos del estudio que la cuenta del licenciado Luis García había sido hackeada y que información confidencial podría estar comprometida.

El mismo día, intenté acceder a mi carpeta compartida en el servidor central, pero el acceso estaba restringido. Informé de esto a Raúl Jiménez, quien me dijo que estaban haciendo mantenimiento, lo que me pareció extraño. Posteriormente, el 8 de octubre, al revisar los archivos de mi computadora, noté que algunos de mis contratos confidenciales tenían marcas de edición que yo no había realizado.

Este incidente me tiene muy preocupado, ya que manejo contratos de gran valor económico y estratégico. No descarto que esto pueda derivar en una fuga de información hacia competidores.

6. Testimonio de Daniela Torres Rivas, practicante de segundo año

Fecha: 23 de octubre de 2023.

Lugar: Sala de juntas del Estudio Jurídico García & Asociados.

El 2 de octubre de 2023, estaba trabajando en mi computadora cuando noté que mis archivos se abrían automáticamente. Creí que era un problema técnico, pero no le di mayor importancia. Días después, el 5 de octubre, intenté abrir una carpeta donde guardo los borradores de los escritos jurídicos que desarrollo, pero no estaba accesible. Más tarde ese mismo día, el jefe de TI, Raúl Jiménez, me preguntó qué tipo de información almacenaba en mi carpeta personal, lo que me pareció muy invasivo. El 7 de octubre, una compañera me mencionó que algunos mensajes internos del chat de trabajo habían sido extraídos y mostrados en una reunión privada de Recursos Humanos. Esto me hizo sospechar que alguien podría estar monitoreando nuestras actividades.

Estoy preocupada por la posibilidad de que hayan accedido a información personal o confidencial sin mi consentimiento.

7. Testimonio de Carlos Hernández Vega, practicante recién ingresado

Fecha: 24 de octubre de 2023.

Lugar: Oficina de Recursos Humanos.

El 4 de octubre de 2023, recibí un correo en mi bandeja de entrada con el asunto 'Urgente: actualización de software'. El remitente parecía legítimo porque incluía el logotipo de nuestro proveedor de software. Al abrir el archivo adjunto, mi computadora se congeló y apareció un mensaje diciendo que mi equipo estaba bloqueado.

Informé de inmediato al jefe de TI, quien dijo que iba a revisar el asunto, pero al día siguiente, el 5 de octubre, el servidor central de la firma también fue afectado. Nos enteramos de que toda la información estaba cifrada y que el atacante estaba pidiendo un rescate en bitcoins. Me siento muy culpable por lo que ocurrió, pero jamás pensé que abrir un archivo pudiera causar tanto daño.

8. Testimonio de Raúl Jiménez Cruz, jefe de TI

Fecha: 25 de octubre de 2023.

Lugar: Oficina de TI.

A finales de septiembre de 2023, Beatriz Sánchez, la jefa de Recursos Humanos, me pidió instalar un software de monitoreo en las computadoras del personal. Justificó esto diciendo que necesitaba evaluar la productividad. Instalé el programa el 1 de octubre en todos los equipos de la red interna.

El 4 de octubre, fui notificado por Carlos Hernández de que su computadora había sido infectada. Al revisar los sistemas, descubrí que un ransomware se había extendido por la red. Traté de contenerlo, pero para el 5 de octubre ya había comprometido el servidor central. Sé que las acciones tomadas con el software de monitoreo fueron inapropiadas, pero jamás pensé que algo así podría pasar.

9. Testimonio de Beatriz Sánchez Flores, jefa de Recursos Humanos

Mi intención al solicitar la instalación del software de monitoreo el 1 de octubre de 2023 era exclusivamente para mejorar el control interno. Lo consulté verbalmente con el licenciado Luis García, quien no se opuso. Sin embargo, reconozco que nunca solicité un consentimiento por escrito del personal.

Me sorprendió mucho cuando el 5 de octubre, se me informó que la red del estudio estaba comprometida. Siento que mis acciones pudieron haber contribuido, aunque mi intención nunca fue perjudicar a nadie.

10. Testimonio de Marta López Núñez, secretaria

Fecha: 26 de octubre de 2023.

Lugar: Sala de juntas del Estudio Jurídico García & Asociados.

El 3 de octubre de 2023, al revisar mi correo corporativo en la mañana, noté que había recibido un mensaje extraño con el asunto 'Actualización de seguridad urgente'. No le di importancia y lo eliminé. Ese mismo día, durante mi horario de almuerzo, escuché a Carlos Hernández hablando con un compañero sobre un correo similar que él sí había abierto.

El 5 de octubre, cuando intenté acceder al servidor para buscar información sobre los casos en curso, mi computadora mostró un mensaje de error. Más tarde nos informaron que el servidor central había sido bloqueado y que el estudio estaba siendo extorsionado.

Además, noté que los correos internos de varios empleados, incluida la licenciada María Ortega, estaban siendo reenviados automáticamente a una dirección desconocida. Informé de esto al jefe de TI, pero no recibí una respuesta clara. También recuerdo haber escuchado una discusión entre Raúl Jiménez y Beatriz Sánchez días antes del incidente, aunque no sé exactamente de qué hablaban.

11. Testimonio de Sofía Morales Díaz, cliente

Fecha: 27 de octubre de 2023.

Lugar: Oficina de clientes del Estudio Jurídico García & Asociados.

El 5 de octubre de 2023, por la tarde, recibí un mensaje en mi teléfono móvil que decía: 'Su caso no es tan privado como piensa. Si desea mantenerlo en secreto, necesitamos que coopere'. Al principio pensé que era un intento de estafa, pero al ver

las noticias al día siguiente, entendí que la firma había sido víctima de un ataque informático. Esto me preocupó mucho, ya que mi caso de divorcio contiene detalles muy sensibles sobre mis bienes y mi vida personal.

Ese mismo día llamé al licenciado Jorge Martínez, quien es mi contacto principal en el estudio, para preguntar si la información de mi caso estaba segura. No pudo confirmarme nada, lo cual me dejó muy intranquila. Desde entonces, he recibido otros mensajes sospechosos y llamadas de números desconocidos.

Confío en que la firma hará todo lo posible para proteger la confidencialidad de sus clientes, pero necesito respuestas claras sobre qué información pudo haberse filtrado.

12. Testimonio de Fernando Álvarez Soto, cliente corporativo

Fecha: 28 de octubre de 2023.

Lugar: Sala de juntas del Estudio Jurídico García & Asociados.

El 7 de octubre de 2023, recibí una llamada desde un número desconocido. Una voz masculina me dijo que tenían acceso a un contrato confidencial entre mi empresa y un proveedor estratégico. Me pidió tres bitcoins como pago para no divulgar el documento. Me sorprendí porque este contrato solo estaba almacenado en los servidores del estudio.

Inmediatamente llamé al licenciado Luis García para informarle de la situación. Él me explicó que el estudio había sufrido un ataque informático, pero no pudo garantizarme que la información de mi empresa estuviera completamente protegida. Esto ha generado una gran preocupación, ya que la exposición de estos datos podría costarme millones de pesos en pérdidas.

Hasta el momento, no he pagado el rescate, pero temo que puedan hacer pública la información. Espero que este problema se resuelva rápidamente y que los responsables enfrenten las consecuencias legales.

13. Correo electrónico 1

Recibido por Carlos Hernández Vega, practicante

Fecha: 4 de octubre de 2023

Asunto: Actualización Urgente de Seguridad

De: soporte.ti@seguridadcorporativa.com

Para: carlos.hernandez@garciayasociados.com

Asunto: Actualización Urgente de Seguridad

Estimado Carlos,

Por motivos de seguridad, es imprescindible que actualices el software de tu equipo para garantizar el correcto funcionamiento y proteger la información de la red. Te pedimos descargar e instalar la actualización desde el enlace proporcionado a continuación:

Haga clic aquí para descargar la actualización

Por favor, realiza esta acción antes de las 6:00 p.m. del día de hoy para evitar interrupciones en el acceso a los recursos del servidor.

Gracias por tu colaboración.

Atentamente,

Equipo de Soporte TI

[Nota: Este mensaje es automático, por favor no respondas.]

14. Correo electrónico 2

Recibido por Sofía Morales Díaz, cliente

Fecha: 5 de octubre de 2023

Asunto: Información Confidencial Comprometida

De: confidencial@protegemosdatos.com

Para: sofia.morales@ejemplo.com

Asunto: Información Confidencial Comprometida Sra. Morales:

Hemos tenido acceso a información muy sensible relacionada con su caso en curso en el Estudio Jurídico García & Asociados. Si no desea que esta información sea divulgada, deberá transferir $15,000 USD en criptomonedas (equivalente a 0.42 bitcoins) a la siguiente dirección: bc1q2x3y4z5abcd678910efghijklmn

Tiene un plazo de 72 horas para realizar el pago. De no recibirlo, tomaremos acciones definitivas que podrían comprometer su privacidad.

Cualquier intento de contactar a las autoridades o al estudio agravará la situación.

Atentamente,

Equipo de Protección de Información

15. Informe técnico de incidencia

Elaborado por: Ing. Alejandro Ruiz Gómez

Fecha: 10 de octubre de 2023

Destinatario: Lic. Luis García López

Asunto: Informe Técnico sobre Incidencia de Seguridad Informática

a. Descripción del incidente

El 4 de octubre de 2023, un correo malicioso fue recibido por uno de los empleados del Estudio Jurídico García & Asociados. Al abrir el archivo adjunto, el equipo del usuario fue infectado con un malware del tipo ransomware. Esto permitió a los atacantes cifrar el servidor central del estudio, comprometiendo toda la información almacenada, incluidos documentos confidenciales de clientes y archivos internos.

b. Hallazgos principales

- Correo de phishing: El malware fue introducido mediante un correo electrónico que simulaba ser de un proveedor de servicios de TI. El remitente utilizó técnicas de ingeniería social, incluyendo un dominio falso (@seguridadcorporativa.com) para ganar credibilidad.
- Ransomware identificado: El ataque fue perpetrado por una variante del ransomware LockBit 3.0, conocido por cifrar rápidamente grandes volúmenes de datos y exigir rescates en criptomonedas.

- Compromiso de la red interna: Una vez infectado el equipo inicial, el ransomware se propagó utilizando vulnerabilidades no parcheadas en la red interna.
- Falta de segmentación de la red: La ausencia de controles adecuados permitió que el ataque afectara tanto a estaciones de trabajo individuales como al servidor principal.
- Monitoreo no autorizado: También se detectó la instalación de un software espía en varias estaciones de trabajo, ejecutado sin el consentimiento de los empleados. Este software recolectaba información confidencial y probablemente facilitó la escalada del ataque.

c. Impacto

- Cifrado del servidor central: Todos los datos en el servidor están inaccesibles.
- Exposición de datos confidenciales: Existe un alto riesgo de que documentos sensibles de clientes hayan sido extraídos antes del cifrado.
- Demanda de rescate: El atacante exige 3 bitcoins (aproximadamente $85,000 USD al tipo de cambio actual).

d. Recomendaciones

- *No pagar el rescate: Aunque pagar puede parecer una solución rápida, no garantiza la recuperación de los datos ni la eliminación de las copias en poder del atacante.*
- *Contratar un equipo especializado en recuperación de ransomware: Se debe intentar recuperar la infor mación a través de técnicas de desencriptado y copias de seguridad.*
- *Fortalecer la seguridad de la red: Implementar segmentación de red, protocolos de doble autenticación, y un sistema de detección de intrusos.*
- *Capacitación del personal: Realizar talleres sobre ciberseguridad para prevenir futuros ataques de phishing.*
- *Auditoría externa: Contratar una firma especializada para evaluar el nivel de compromiso actual y prevenir nuevos incidentes.*

e. Conclusión

El incidente actual evidencia deficiencias graves en la infraestructura de seguridad del Estudio Jurídico García & Asociados. Se recomienda actuar de inmediato para mitigar los riesgos presentes y prevenir futuros ataques.

Atentamente,

Ing. Alejandro Ruiz Gómez

Consultor en Ciberseguridad

BIBLIOGRAFÍA



* La ilustración de la página anterior corresponde a una adaptación de "Caballero elegante en la biblioteca" de Johan Hamza. Para su elaboración se empleó OpenAI.

BIBLIOGRAFÍA

Sumario: A. Fuentes impresas. B. Fuentes electrónicas. C. Legislación y otros documentos legales. D. Fuentes jurisprudenciales

A. FUENTES IMPRESAS

Aboso, Gustavo Eduardo. *Derecho penal cibernético: La cibercriminalidad y el derecho penal en la moderna sociedad de la información y la tecnología de la comunicación*. Montevideo: B de F, 2018.

Aboso, Gustavo Eduardo. "Acceso indebido a las comunicaciones electrónicas en el ámbito laboral". En: Dupuy, Daniela (dir.) y Mariana Kiefer (coord.). *Cibercrimen. Aspectos de derecho penal y procesal penal. Cooperación internacional. Recolección de evidencia digital. Responsabilidad de los proveedores de servicios de Internet*. Montevideo: B de F, 2019.

Aboso, Gustavo Eduardo y María Florencia Zapata. *Cibercriminalidad y derecho penal. La información y los sistemas informáticos como nuevo paradigma del derecho penal. Análisis doctrinario, jurisprudencial y derecho comparado sobre los denominados delitos informáticos*. Montevideo: B de F, 2006.

Almanza Altamirano, Frank. *Cibercriminalidad y nuevas modalidades delictivas*. Lima: San Bernardo, 2024.

Ambos, Kai. *Responsabilidad penal internacional en el ciberespacio*. Bogotá: Universidad Externado de Colombia, 2014.

Angulo Aguirre, Luis. *Hacking & cracking. Redes inalámbricas Wi-Fi*. Lima: Macro, 2018.

Arévalo Minchola, Maguín y J. A. Vega Aguilar, *Ciberdelitos. Análisis en el sistema penal.* Lima: Iustitia, 2022.

Arocena, Gustavo Eduardo. "Cibercrimen. Aproximaciones y una breve referencia a la legislación argentina". En: Caro Coria, Carlos Dino y Luis Reyna Alfaro (dirs.). *Ciberseguridad, cibercrimen y nuevas tecnologías. Riesgos y respuestas jurídicas.* Ciudad de México: Derecho Global Editores, 2022.

Arthur, Charles. *Cyber Wars. Hackeos que hicieron temblar el mundo empresarial.* Zaragoza: Teell, 2019.

Asencio Gallego, José María. "Los delitos informáticos y las medidas de investigación y obtención de pruebas en el Convenio de Budapest sobre la ciberdelincuencia". En: Asencio Mellado, José María (dir.). *Justicia penal y nuevas formas de delincuencia.* Valencia: Tirant lo Blanch, 2017.

Asociación Mundial de Derecho Penal. "XV Congreso Internacional de derecho penal". En: *Anuario de Derecho Penal y Ciencias Penales* 1. Madrid: 1995.

Atienza, Manuel. *Argumentación legislativa.* Buenos Aires: Astrea, 2019.

Bachmaier Winter, Lorena. "Registro remoto de equipos informáticos en la Ley Orgánica 13/2015: Algunas cuestiones sobre el principio de proporcionalidad". En: Cedeño Hernán, Marina. *Nuevas tecnologías y derechos fundamentales en el proceso.* Navarra: Thomson Reuters / Aranzadi, 2017.

Barrio Andrés, Moisés. *Delitos 2.0. Aspectos penales, procesales y de seguridad de los ciberdelitos.* Madrid: Wolters Kluwer, 2018.

Barrio Andrés, Moisés. *Fundamentos del derecho de internet.* 2.ª edición. Madrid: Centro de Estudios Políticos y Constitucionales, 2020.

Blossiers Hüme, Juan José. *Criminalidad informática.* Lima: Editorial Portocarrero, 2003.

Bramont-Arias Torres, Luis Alberto. *El delito informático en el Código Penal peruano.* Lima: Pontificia Universidad Católica del Perú, 1997.

Brodowski, Dominik. *Cibercrimen y protección de la seguridad informática.* Buenos Aires: Ad-Hoc, 2021.

Caballero, María Ángeles y Diego Cilleros Serrano. *El libro del hacker. Edición 2022*. Madrid: Anaya, 2022.

Castillo Alva, José Luis. "Finalidad del Código Penal". En: Salazar Sánchez, Nelson (dir.). *Comentarios al Código Penal peruano. Parte general*, t. I. Lima: Gaceta Jurídica, 2019.

Coleman, Gabriella. *Las mil caras de Anonymous. Hackers, activistas, espías y bromistas*. Barcelona: Arpa y Alfil, 2016.

Contreras, Cristian. *La valoración de la prueba de interrogatorio*. Madrid: Marcial Pons, 2015.

Contreras, Paul. *Me llamo Kohfman. Identidad hacker: una aproximación antropológica*. Barcelona: Gedisa, 2004.

Corcoy Bidasolo, Mirentxu. "Protección penal del sabotaje informático. Especial consideración de los delitos de daños". En: Mir Puig, Santiago (coord.). *Delincuencia informática*. Barcelona: PPU, 1992.

Daswani, Deepak. *La amenaza hacker. Todo lo que empresarios, directivos, profesionales y particulares deberíamos saber para protegernos adecuadamente*. Barcelona: Deusto, 2018.

Davara Fernández de Marcos, Elena y Laura Davara Fernández de Marcos (coords.). *Delitos informáticos*. Navarra: Thomson Reuters / Aranzadi, 2017.

De La Mata Barranco, Norberto. "Reflexiones sobre el bien jurídico a proteger en el delito de acceso ilícito (art. 197 bis CP). El concepto de privacidad informática y la tutela del buen funcionamiento de los sistemas de información y comunicación". En: *Cuadernos de Política Criminal* 118. Madrid: 2016.

De La Mata Barranco, Norberto. "La tutela de la integridad y disponibilidad de datos y sistemas informáticos: El modelo tradicional vinculado a una protección estrictamente patrimonial, un mal referente". En: Riquert, Marcelo A. (dir.) y Carlos Christian Sueiro (coord.). *Sistema penal e informática. Ciberdelitos. Evidencia digital. TICS*, vol. 1. Buenos Aires: Hammurabi, 2019.

De La Rosa Rodríguez, Paola Iliana. *Las tecnologías, el ciberespacio y el derecho penal. Estudios sobre la prueba científica y la prueba electrónica.* Ciudad de México: Porrúa, 2019.

Del Carril, Enrique H. "Desafíos del cibercrimen para el Derecho internacional". En: Dupuy, Daniela (dir.). *Cibercrimen II. Nuevas conductas penales y contravencionales. Inteligencia artificial aplicada al derecho penal y procesal penal. Novedosos medios probatorios para recolectar evidencia digital. Cooperación internacional y victimología.* Montevideo: B de F, 2018.

Díaz Colchado, Juan y Andreé Castro Arequipeño. "Los derechos fundamentales y las nuevas tecnologías de la información y comunicación: Una aproximación". En: *Thémis* 79. Lima: 2021.

Duffy, Bobby. *El mito de las generaciones. Por qué cuándo naciste importa menos de lo que piensas.* Madrid: Urano, 2022.

Dupuy, Daniela (dir.). *Cibercrimen II. Nuevas conductas penales y contravencionales. Inteligencia artificial aplicada al derecho penal y procesal penal. Novedosos medios probatorios para recolectar evidencia digital. Cooperación internacional y victimología.* Montevideo: B de F, 2018.

Dupuy, Daniela. "Ciberdelitos: desafíos para trabajar". En: Vanessa Y. Ferrazzuolo (coord.). *Era digital: delito y prevención.* Buenos Aires: Jusbaires, 2019.

Dupuy, Daniela y Mariana Kiefer. "Datos e innovación tecnológica". En: Dupuy, Daniela (dir.). *Cibercrimen III. Inteligencia artificial. Automatización, algoritmos y predicciones en el derecho penal y procesal penal.* Montevideo: B de F, 2022.

Durand Valladares, Raúl. "Los delitos informáticos en el Código Penal peruano". En: *Revista Peruana de Ciencias Penales* 11. Lima: 2002.

Elías Puelles, Ricardo. "Daños y sabotajes informáticos: ataques contra los datos y los sistemas informáticos". En: Caro Coria, Carlos; Luis Miguel Reyna Alfaro y Ricardo Elías Puelles (dirs.). *Ciberseguridad, cibercrimen, y AI LegalTech.* México: Derecho Global Editores, 2025.

Elías Puelles, Ricardo. "El delito de *hacking* o acceso ilícito a sistemas informáticos". En: *Thémis* 83, Lima: 2023.

Elías Puelles, Ricardo. "La evolución del cibercrimen en el Perú. De hurto telemático a ataques contra sistemas informáticos". En: Espinoza Calderón, Víctor Raúl (coord.). *Cibercriminalidad y delitos informáticos*. Lima: Instituto Pacífico, 2023.

Elías Puelles, Ricardo. "Luces y sombras en la lucha contra la delincuencia informática en el Perú". En: Dupuy, Daniela (dir.) y Mariana Kiefer (coord.). *Cibercrimen. Aspectos de derecho penal y procesal penal. Cooperación internacional. Recolección de evidencia digital. Responsabilidad de los proveedores de servicios de Internet*. Montevideo: B de F, 2019.

Espinoza Calderón, Víctor Raúl. *Delitos informáticos y nuevas modalidades delictivas*. Lima: Instituto Pacífico, 2022.

Espinoza Calderón, Víctor Raúl (coord.). *Cibercriminalidad y delitos informáticos*. Lima: Instituto Pacífico, 2023.

Estévez, José Francisco y Elena Santos. "Ciberdelitos y ciberseguridad". En: Estévez, José (dir.). *Derecho digital*. Navarra: Thomson Reuters / Aranzadi, 2019.

Eve, Martin Paul. *Una historia de las contr43eñ4s*. Buenos Aires: Godot, 2023.

Fariña, Cristian; Alexis Blasco y Fernando Dedovich. "Legislación comparativa sobre cibercrimen en Latinoamérica". En: Dupuy, Daniela (dir.) y Mariana Kiefer (coord.). *Cibercrimen. Aspectos de derecho penal y procesal penal. Cooperación internacional. Recolección de evidencia digital. Responsabilidad de los proveedores de servicios de Internet*. Montevideo: B de F, 2019.

Ferrazzuolo, Vanessa Y. (coord.). *Era digital: delito y prevención*. Buenos Aires: Jusbaires, 2019.

Flores Prada, Ignacio. *Criminalidad informática: aspectos sustantivos y procesales*. Valencia: Tirant lo Blanch, 2012.

Fusalba, Joana y Javier Martín López Zavaleta. "Los registros domiciliarios con análisis de dispositivos de almacenamiento de datos en el lugar. Qué ocurre en las investigaciones de delitos que involucran la integridad sexual de menores. Realidad judicial y la implicancia de la adhesión de la República de Argentina al Convenio de Budapest sobre ciberdelincuencia. Necesidad de reformas procesales". En: Dupuy, Daniela (dir.) y Mariana

Kiefer (coord.). *Cibercrimen II. Nuevas conductas penales y contravencionales. Inteligencia artificial aplicada al derecho penal y procesal penal. Novedosos medios probatorios para recolectar evidencia digital. Cooperación internacional y victimología*. Montevideo: B de F, 2018.

Garat, Sebastián y Julián Reale. "La reforma penal en materia de cibercrimen en la República de Argentina". En: Dupuy, Daniela (dir.). *Cibercrimen II. Nuevas conductas penales y contravencionales. Inteligencia artificial aplicada al derecho penal y procesal penal. Novedosos medios probatorios para recolectar evidencia digital. Cooperación internacional y victimología*. Montevideo: B de F, 2018.

García Cavero, Percy. *Derecho penal económico. Parte general*. 4.ª edición. Lima: Instituto Pacífico, 2022.

García León, Godofredo André. "Análisis del tipo de acceso ilícito. Bien jurídico, tipicidad objetiva y subjetiva, autoría y participación, y su distinción con el delito de atentado a la integridad de datos y sistemas informáticos". En: Espinoza Calderón, Víctor Raúl (coord.). *Cibercriminalidad y delitos informáticos*. Lima: Instituto Pacífico, 2023.

García-Pablos De Molina, Antonio. *Derecho penal. Parte general: Fundamentos*. Lima: Jurista Editores, 2009.

Gil Gil, Alicia y Roberto Hernández Berlinches (coords.), *Cibercriminalidad*. Madrid: Dykinson, 2019.

Gil Gil, Alicia. "Daños informáticos". En: Sanz Delgado, Enrique y Daniel Fernández Bermejo (coords.) *Tratado de delincuencia cibernética*. Navarra: Thomson Reuters / Aranzadi, 2021.

Goodman, Marc. *Los delitos del futuro. Todo está conectado. Todos somos vulnerables. ¿Qué podemos hacer al respecto?* Barcelona: Ariel, 2019

Grabosky, Peter. *Cybercrime. Keynotes in Criminology and Criminal Justice Series*. New York: Oxford University Press, 2016.

Gutiérrez de Aizpuru, Julia. "Implicaciones legales de las redes sociales". En: Estévez, José (dir.). *Derecho digital*. Navarra: Thomson Reuters, 2019.

Hernández Díaz, Leyre. "La regulación penal del hacking blanco: el modelo del Código Penal español". En: Caro Coria, Carlos Dino y Luis Reyna Alfaro (dirs.). *Ciberseguridad, cibercrimen y nuevas tecnologías. Riesgos y respuestas jurídicas*. Ciudad de México: Derecho Global Editores, 2022.

Hernández Díaz, Leyre. *Los accesos ilícitos a sistemas informáticos. Normativa internacional y regulación en el ordenamiento penal español*. Navarra: Thomson Reuters / Aranzadi, 2019.

Jiménez Herrera, Juan Carlos. *Manual de derecho penal informático*. Lima: Jurista, 2017.

Johnson, Ann. "Los profesionales de InfoSec deben aplicar la resiliencia operativa". En: Morillo, Christina (ed.). *97 cosas que todo profesional de la seguridad informática debería saber*. Madrid: Grupo Anaya, 2022.

Kenyon, Henry. "The network of our times. A DARPA perspective on the development of the internet". En: *DARPA. Defense Advanced Research Projects Agency, 1958-2018*. Tampa (FL.): Faircount Media Group, 2018. https://www.darpa.mil/sites/default/files/attachment/2025-02/magazine-darpa-60th-anniversary.pdf

Kiefer, Mariana. "Daño informático". En: Dupuy, Daniela (dir.) y Mariana Kiefer (coord.). *Cibercrimen. Aspectos de derecho penal y procesal penal. Cooperación internacional. Recolección de evidencia digital. Responsabilidad de los proveedores de servicios de Internet*. Montevideo: B de F, 2019.

Kremling, Janine y Amanda M. Sharp Parker. *Cyberspace, Cybersecurity, and Cybercrime*. Thousand Oaks: Sage Publications, 2017.

Lavorgna, Anita. *Cybercrimes. Critical issues in a global context*. Londres: Red Globes Press, 2020.

Lledó Benito, Ignacio. *Formas específicas de criminalidad*. Madrid: Dykinson, 2019.

Marcum, Catherine D. *Cyber crime*. 2.ª edición. New York: Wolters Kluwer, 2019.

Martínez Alba, Flores. "La transformación digital del dato: nuevos usos y nuevos métodos". En: Perea Ortega, Rafael (dir.). *Estudios sobre derecho digital*. Navarra: Thomson Reuters / Aranzadi, 2021.

Martínez Zorrilla, David. *Metodología jurídica y argumentación.* Madrid: Marcial Pons, 2010.

Mazuelos Coello, Julio F. "Los delitos informáticos: Una aproximación a la regulación del Código Penal peruano". En: *Revista Peruana de Doctrina y Jurisprudencia Penales* 2. Lima: Grijley, 2001.

Mazzoni, Giuliana. *¿Se puede creer a un testigo? El testimonio y las trampas de la memoria.* Madrid: Trotta, 2010.

Mendiguri Peralta, David Rosario. *El dolo como magnitud graduable: Cómo determinar la pena según la intensidad del dolo. Análisis doctrinario y jurisprudencial.* Lima: Instituto Pacífico, 2024.

Menéndez Mato, Juan Carlos y María Eugenia Gayo Santa Cecilia. *Derecho e informática. Ética y legislación.* Barcelona: Bosch, 2014.

Meneses Gonzáles, Bonifacio y Jean Paul Meneses Ochoa. *La cibercriminalidad: Consideración criminológica, político-criminal, dogmática, procesal y cooperación internacional.* Salamanca: UPSA, 2024.

Messdaghi, Chloé. "Cuatro aspectos importantes de ciberseguridad". En: Morillo, Christina (ed.). *97 cosas que todo profesional de la seguridad informática debería saber.* Madrid: Grupo Anaya, 2022.

Mestre Delgado, Esteban. "Introducción. Nuevas respuestas legales y jurisprudenciales frente a nuevas formas de criminalidad". En: Sanz Delgado, Enrique y Daniel Fernández Bermejo. *Tratado de delincuencia cibernética.* Navarra: Thomson Reuters / Aranzadi, 2021.

Mir Puig, Santiago. *Derecho penal. Parte general.* 6.ª edición (2.ª reimpresión). Barcelona: Reppertor, 2008.

Miró Llinares, Fernando. *El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio.* Madrid: Marcial Pons, 2012.

Möhrenschlager, Manfred E. "El nuevo derecho penal informático en Alemania". En: Mir Puig, Santiago (coord.). *Delincuencia informática.* Barcelona: PPU, 1992.

Möhrenschlager, Manfred E. "Tendencias en política jurídica en la lucha contra la delincuencia relacionada con la Informática". En: Mir Puig, Santiago (coord.). *Delincuencia informática.* Barcelona: PPU, 1992.

Montoya Piña, Javier Omar. *Delitos federales cometidos a través de medios informáticos.* México D.F.: Flores Editores y Distribuidores, 2015.

Montserrat Sánchez-Escribano, María Isabel. *El delito de acceso ilícito a un sistema informático: aspectos relativos a su regulación e interpretación.* Navarra: Thomson Reuters / Aranzadi, 2022.

Morachimo Rodríguez, Miguel. "Deconstruyendo la ley de delitos informáticos". En: *Gaceta Constitucional* 71, Lima: 2013.

Morillo, Christina (ed.). *97 cosas que todo profesional de la seguridad informática debería saber.* Madrid: Grupo Anaya, 2022.

Morón Lerma, Esther. *Internet y derecho penal: "Hacking" y otras conductas ilícitas en la red.* Navarra: Thomson Reuters / Aranzadi, 1999.

Muñoz Conde, Francisco y Mercedes García Arán. *Derecho penal. Parte general.* 7.ª edición, revisada y puesta al día. Valencia: Tirant lo Blanch, 2007.

Nava Garcés, Alberto. *Delitos informáticos.* 4.ª edición. México: Porrúa, 2018.

Nieva Fenoll, Jordi. *La valoración de la prueba.* Madrid: Marcial Pons, 2010.

Nycum, Susan Hubell. "Legal problems of computer abuse". En: *Washington University Law Review* 3, 1977. https://journals.library.wustl.edu/lawreview/article/2231/galley/19064/view/

Oré Sosa, Eduardo. *Delictum. Apuntes de derecho penal.* Lima: Editores del Centro, 2022.

Organisation for Economic Co-Operation and Development. "Computer crime". En: *The OECD Observer* 142, septiembre. Paris: 1986.

Ortiz Hernández, Susana. "La regulación de los delitos con origen tecnológico". En: Garrós Font, Imma y otros. *Delitos cibernéticos: amenazas digitales del siglo XXI. Análisis normativo, psicológico y criminológico.* Navarra: Thomson Reuters / Aranzadi, 2023.

Ortiz Pradillo, Juan Carlos. "Comunicaciones, tecnología y proceso penal. Viejos delitos, nuevas necesidades". En: Asencio Mellado, José María (dir.). *Justicia penal y nuevas formas de delincuencia.* Valencia: Tirant lo Blanch, 2017.

Palazzi, Pablo A. "El delito de acceso ilegítimo a un sistema informático". En: Dupuy, Daniela (dir.). *Cibercrimen II. Nuevas conductas penales y contravencionales. Inteligencia artificial aplicada al derecho penal y procesal penal. Novedosos medios probatorios para recolectar evidencia digital. Cooperación internacional y victimología.* Buenos Aires: B de F, 2018.

Palomá Parra, Luis Orlando. *La organización. Modalidades del crimen en el ciberespacio.* Bogotá: Grupo Editorial Ibáñez, 2021.

Palomino Ramírez, Walter. "El intrusismo y los otros delitos informáticos regulados en la Ley N.° 30096". En: *Gaceta Penal & Procesal Penal* 56. Lima: 2014.

Paricio, Javier, Idoia Fernández y Amparo Fernández. "Una concepción de la docencia problemática, compleja y basada en la investigación". En: Paricio, Javier *et al. Cartografía de la buena docencia universitaria. Un marco para el desarrollo del profesorado basado en la investigación.* Madrid: Narcea, 2019.

Parker, Donn B. *Computer Crime: Criminal Justice Resource Manual.* Washington D. C.: National Institute of Justice, 1989.

Peña Cabrera Freyre, Alonso. "Los delitos informáticos: el uso de instrumentos digitales en las redes informáticas y en el ciberespacio". En: *Gaceta Penal & Procesal Penal* 76. Lima: 2015.

Perea Ortega, Rafael (dir.). *Estudios sobre derecho digital.* Navarra: Thomson Reuters / Aranzadi, 2021.

Pérez López, Jorge. *Delitos regulados en leyes penales especiales.* Lima: Gaceta Jurídica, 2019.

Pérez-Prat Durbán, Luis. "Los ciberataques y el uso de la fuerza en las relaciones internacionales". En: Millán Moro, Lucía (dir.). *Ciberataques y ciberseguridad en la escena internacional.* Navarra: Thomson Reuters / Aranzadi, 2019.

Piernas López, Juan Jorge. "La respuesta de la Unión Europea a las amenazas del ciberespacio". En: Cervell Hortal, María José (Dir). *Nuevas tecnologías en el uso de la fuerza: Drones, armas autónomas y ciberespacio.* Navarra: Thomson Reuters / Aranzadi, 2020.

Pillado Quintas, Víctor. "Las medidas de investigación tecnológica. Visión del ministerio fiscal". En: Pereira Puigvert, Sílvia y Francesc Ordóñez Ponz (dirs.) *Investigación y proceso penal en el Siglo XXI, nuevas tecnologías y protección de datos*. Cizur Menor: Thomson Reuters / Aranzadi, 2021.

Pons, Anaclet. *El desorden digital. Guía para historiadores y humanistas*. Madrid: Siglo XXI, 2013.

Posada Maya, Ricardo. *Los cibercrímenes: Un nuevo paradigma de criminalidad. Un estudio del título VII bis del Código Penal colombiano*. Bogotá: Grupo Editorial Ibáñez, 2017.

Quian, Alberto. *Civilización hacker*. Madrid: Grupo Anaya, 2022.

Quintana, Yolanda. *Ciberguerra*. Madrid: Los Libros de la Catarata, 2016.

Raboy, Marc. *Marconi: The man who networked the world*. New York: Oxford University Press, 2016.

Reale, Julián M. "Importancia de la instrumentalización jurídica de la *vulnerability assessment* y la etapa de explotación de vulnerabilidades para evitar su criminalización". En: Salt, Marcos G. (Dir). *@UBACibercrimen | 1*. Buenos Aires: Ad-Hoc, 2022.

Requejo Passoni, Wendy. "Avances y retrocesos de la política criminal relativa a los delitos contra datos y sistemas informáticos en el Perú". En: Caro Coria, Carlos Dino y Luis Reyna Alfaro (dir.). *Ciberseguridad, cibercrimen y nuevas tecnologías. Riesgos y respuestas jurídicas*. Ciudad de México: Derecho Global Editores, 2022.

Reyna Alfaro, Luis. "Litigación y persuasión *on streaming*. Una aproximación a los retos de la justicia virtual". En: *Gaceta de Litigación Penal* 3, noviembre-diciembre. Lima: 2021.

Reyna Alfaro, Luis. *Los delitos informáticos: Aspectos criminológicos, dogmáticos y de política criminal*. Lima: Jurista, 2002.

Riquert, Marcelo A. *Delincuencia informática en Argentina y el Mercosur*. Buenos Aires: Ediar, 2009.

Riquert, Marcelo (coord.). *Ciberdelitos: Grooming, stalking, bullying, sexting, ciberodio, propiedad intelectual, problemas de perseguibilidad, ciberpornografía infantil.* Buenos Aires: Hammurabi, 2014.

Riquert, Marcelo A. "La responsabilidad penal de las personas jurídicas en Argentina y el ciberconvenio de Budapest". En: Dupuy, Daniela (dir.). *Cibercrimen II. Nuevas conductas penales y contravencionales. Inteligencia artificial aplicada al derecho penal y procesal penal. Novedosos medios probatorios para recolectar evidencia digital. Cooperación internacional y victimología.* Montevideo: B de F, 2018.

Riquert, Marcelo A. (dir.) y Carlos Christian Sueiro (coord.). *Sistema penal e informática. Ciberdelitos. Evidencia digital. TICS*, vol. 1. Buenos Aires: Hammurabi, 2019.

Riquert, Marcelo A. "El acceso ilegítimo a sistema o dato informático (art. 153 bis del Código Penal)". En: Dupuy, Daniela (dir.) y Mariana Kiefer (coord.). *Cibercrimen. Aspectos de derecho penal y procesal penal. Cooperación internacional. Recolección de evidencia digital. Responsabilidad de los proveedores de servicios de Internet.* Montevideo: B de F, 2019.

Rodríguez Rocha, Lizet Nancy. "El delito de acceso ilícito a los sistemas informáticos. Análisis del tipo penal y el rol de la cooperación judicial internacional". En: Espinoza Calderón, Víctor Raúl (coord.). *Cibercriminalidad y delitos informáticos.* Lima: Instituto Pacífico, 2023.

Rojas Vargas, Fidel. *Código Penal. Parte general. Comentarios y jurisprudencia.* Lima: RZ, 2016.

Rovira del Canto, Enrique. *Delincuencia informática y fraudes informáticos.* Granada: Comares, 2002.

Roxin, Claus. *Derecho penal parte general.* T. II: *Especiales formas de aparición del delito.* Navarra: Thomson Reuters / Aranzadi, 2014.

Rubio Correa, Marcial. *El sistema jurídico. Introducción al derecho.* 8.ª edición corregida y aumentada. Lima: Pontificia Universidad Católica del Perú, 1999.

Rueda Martín, María Ángeles. "Cuestiones político-criminales sobre las conductas de *hacking*". En: *Derecho Penal Contemporáneo. Revista Internacional* 28. Bogotá: 2009.

SAIN, Gustavo Raúl. *Delitos y nuevas tecnologías. Fraude, narcotráfico y lavado de dinero por internet.* Buenos Aires: Editores del Puerto, 2012.

SAIN, Gustavo y Horacio AZZOLIN. *Delitos informáticos. Investigación criminal, marco legal y peritaje.* Buenos Aires: B de F, 2018.

SALAZAR SÁNCHEZ, Nelson. "Concurso ideal de delitos". En: SALAZAR SÁNCHEZ, Nelson (dir.). *Comentarios al Código Penal peruano. Parte general,* t. III. Lima: Gaceta Jurídica, 2019.

SALINAS SICCHA, Ramiro. *Derecho penal. Parte especial.* 3.ª edición. Lima: Grijley, 2008.

SALLIS, Ezequiel. "Desafíos de la investigación de los delitos informáticos en la Deep & Dark Web". En: DUPUY, Daniela (dir.) y Mariana KIEFER (coord.). *Cibercrimen. Aspectos de derecho penal y procesal penal. Cooperación internacional. Recolección de evidencia digital. Responsabilidad de los proveedores de servicios de Internet.* Montevideo: B de F, 2019.

SANZ DELGADO, Enrique. "Delincuencia cibernética y descubrimiento y revelación de secretos". En: SANZ DELGADO, Enrique y Daniel FERNÁNDEZ BERMEJO (coords.). *Tratado de delincuencia cibernética.* Navarra: Thomson Reuters / Aranzadi, 2021.

SCHJOLBERG, Stein. *The history of cybercrime.* 3.ª edición. Cybercrime Research Institute, 2020.

SCHWAB, Klaus. *La cuarta revolución industrial.* 8.ª reimpresión, Barcelona: The Penguin Random House, 2023.

SIEBER, Ulrich. "Criminalidad informática: Peligro y prevención". En: MIR PUIG, Santiago (coord.). *Delincuencia informática.* Barcelona: PPU, 1992.

SILVA SÁNCHEZ, Jesús-María. *Derecho penal. Parte general.* Madrid: Civitas, 2025.

STEWART, Camille. "Mantener a las personas en el foco del problema". En: MORILLO, Christina (ed.). *97 cosas que todo profesional de la seguridad informática debería saber.* Madrid: Grupo Anaya, 2022.

SUÁREZ SÁNCHEZ, Alberto. *Manual de delito informático en Colombia. Análisis dogmático de la ley 1273 de 2009,* Universidad Externado de Colombia, Bogotá, 2016.

Sueiro, Carlos Christian. *Casos de criminalidad informática y prueba digital. Casos de inteligencia artificial (IA). Sistematización de jurisprudencia.* Buenos Aires: Ad-Hoc, 2022.

Sueiro, Carlos Christian. *El derecho penal en la era digital. Delincuencia informática. Criminalidad informática. Prueba digital. Vigilancia electrónica. Pedagogía en la era digital.* Lima: A&C, 2018.

Tascón, Mario y Yolanda Quintana. *Ciberactivismo. Las nuevas revoluciones de las multitudes conectadas.* Madrid: Los Libros de la Catarata, 2012.

Tejada De La Fuente, Elvira. "Novedades en la tipificación de determinados delitos vinculados a la criminalidad informática en el Código Penal español: evolución legislativa y adaptación a la normativa internacional". En: Dupuy, Daniela (dir.) y Mariana Kiefer (coord.). *Cibercrimen. Aspectos de derecho penal y procesal penal. Cooperación internacional. Recolección de evidencia digital. Responsabilidad de los proveedores de servicios de Internet.* Montevideo: B de F, 2019.

Temperini, Marcelo y Maximiliano Macedo. "Aspectos legales de la ingeniería social: Análisis de la responsabilidad civil y penal del ingeniero social". En: Riquert, Marcelo A. (dir.) y Carlos Christian Sueiro (coord.). *Sistema penal e informática. Ciberdelitos. Evidencia digital. TICS*, vol. 3. Buenos Aires: Hammurabi, 2020.

Temperini, Marcelo. "Delitos informáticos y cibercrimen: Técnicas y tendencias de investigación penal y su afectación a los derechos constitucionales". En: Dupuy, Daniela (dir.). *Cibercrimen II. Nuevas conductas penales y contravencionales. Inteligencia artificial aplicada al derecho penal y procesal penal. Novedosos medios probatorios para recolectar evidencia digital. Cooperación internacional y victimología.* Montevideo: B de F, 2018.

Torres Blanco, Antoni y otros. "El *hacking* desde una perspectiva legal, criminológica y técnica". En: Garrós Font, Imma *et al. Delitos cibernéticos: amenazas digitales del siglo XXI. Análisis normativo, psicológico y criminológico.* Navarra: Thomson Reuters / Aranzadi, 2023.

Unodc. *Ciberdelito I: Guía práctica para un abordaje integral del fenómeno. Tipos generales. Marco jurídico y derechos humanos. El ABC de la investigación.* Lima: 2022

Vargas Carpio, Mónica Rocío. "Ataques cibernéticos de tipo *ransomware*". En: Espinoza Calderón, Víctor Raúl (coord.). *Cibercriminalidad y delitos informáticos*. Lima: Instituto Pacífico, 2023.

Vargas Carpio, Mónica Rocío. "Atentado a la integridad de datos informáticos (Artículo 3 de la Ley de Delitos Informáticos)". En: Espinoza Calderón, Víctor Raúl (coord.). *Cibercriminalidad y delitos informáticos*. Lima: Instituto Pacífico, 2023.

Velasco Núñez, Eloy. *Delitos tecnológicos. Cuestiones penales y procesales*. Madrid: Wolters Kluwer, 2021.

Velasco Núñez, Eloy y Carolina Sanchís Crespo. *Delincuencia informática. Tipos delictivos e investigación. Con jurisprudencia tras la reforma procesal y penal del 2015*. Valencia: Tirant lo Blanch, 2019.

Velasco San Martín, Cristos. *La jurisdicción y competencia sobre delitos cometidos a través de sistemas de cómputo e internet*. Valencia: Tirant lo Blanch, 2012.

Velasco San Martín, Cristos y Andrés Velázquez. *Aspectos prácticos de los ciberdelitos y la evidencia digital*. Valencia: Tirant lo Blanch, 2021.

Véliz, Carissa. *Privacidad es poder. Datos, vigilancia y libertad en la era digital*. 4.ª reimprensión. Barcelona: Penguin Random House, 2023.

Verdugo Guzmán, Silvia Irene. "Cibercrimen, internet oscura y COVID-19. Inteligencia artificial y transformación digital". En: Madrid Parra, Agustín y Lucía Alvarado Herrera (dirs.) *Derecho digital y nuevas tecnologías*. Navarra: Thomson Reuters / Aranzadi, 2022.

Villanueva, Ernesto y Vanessa Díaz. *Derecho de las nuevas tecnologías (en el siglo XX derecho informático)*. Ciudad de México: Oxford University Press México, 2015.

Villavicencio Terreros, Felipe. "Delitos informáticos". En: *Ius et Veritas* 49. Lima: 2014.

Villavicencio Terreros, Felipe. "Los delitos informáticos en la legislación penal peruana". En: Riquert, Marcelo A. (dir.) y Carlos Christian Sueiro (coord.). *Sistema penal e informática. Ciberdelitos. Evidencia digital. TICS*, vol. 1. Buenos Aires: Hammurabi, 2019.

B. FUENTES ELECTRÓNICAS

BANDLER, John y Antonia MERZON. *Cybercrime investigations. A comprehensive resource for everyone*. Boca Raton: CRC Press, 2020. [Kindle]

BLACK, Edwin. *IBM and the Holocaust. The strategic alliance between Nazi Germany and America's most powerful corporation*. Edición expandida. Washington: Dialog Press, 2012. [e-Book]

BROWN, Thompson. *Essential guide to cybersecurity for beginners and experts: An elementary plan to protect your family and business form cybercrime*. Independently Published. 2021. [Kindle]

CASERO BEJAR, María y María SÁNCHEZ VERA. "Cambio de modalidad presencial a virtual durante el confinamiento por COVID-19: percepciones del alumnado universitario". En: *RIED, Revista Iberoamericana de Educación a Distancia* 25(1). Madrid: 2022. https://www.redalyc.org/journal/3314/331469022015/331469022015.pdf

CENTRO DE POLÍTICA Y DERECHO DE CIBERSEGURIDAD Y UNIVERSIDAD DE DUKE. *Preparación cibernética en los sectores públicos de América Latina: Lecciones de la primera línea*. LATAM CISO Report, 2024. https://es.weforum.org/stories/2024/05/lecciones-de-ciberseguridad-de-la-batalla-de-america-latina-contra-las-amenazas-de-ransomware/

CENTRO NACIONAL DE SEGURIDAD DIGITAL. *Alerta integrada de seguridad digital* N.° 11-2020. Lima: 15 de abril del 2020. https://www.gob.pe/institucion/pcm/informes-publicaciones/544930-alerta-integrada-de-seguridad-digital-n-011-2020-pecert

CENTRO NACIONAL DE SEGURIDAD DIGITAL. *Alerta integrada de seguridad digital* N.° 242-2020. Lima: 2 de diciembre de 2020. https://www.gob.pe/institucion/pcm/informes-publicaciones/1369751-alerta-integrada-de-seguridad-digital-n-242-2020-pecert

CENTRO NACIONAL DE SEGURIDAD DIGITAL. *Alerta integrada de seguridad digital* N.° 23-2021. Lima: 1 de febrero de 2021. https://www.gob.pe/institucion/pcm/informes-publicaciones/1625620-alerta-integrada-de-seguridad-digital-n-023-2021-pecert

Centro Nacional de Seguridad Digital. *Alerta integrada de seguridad digital* N.º 24-2021. Lima: 2 de febrero de 2021. https://www.gob.pe/institucion/pcm/informes-publicaciones/1639099-alerta-integrada-de-seguridad-digital-n-024-2021-pecert

Centro Nacional de Seguridad Digital. *Alerta integrada de seguridad digital* N.º 34-2021. Lima: 13 de febrero de 2021. https://www.gob.pe/institucion/pcm/informes-publicaciones/1683562-alerta-integrada-de-seguridad-digital-n-034-2021-pecert

Centro Nacional de Seguridad Digital. *Alerta integrada de seguridad digital* N.º 47-2021. Lima: 1 de marzo de 2021. https://www.gob.pe/institucion/pcm/informes-publicaciones/1733211-alerta-integrada-de-seguridad-digital-n-047-2021-pecert

Centro Nacional de Seguridad Digital. *Alerta integrada de seguridad digital* N.º 94-2021. Lima: 21 de abril de 2021. https://www.gob.pe/institucion/pcm/informes-publicaciones/1859225-alerta-integrada-de-seguridad-digital-n-094-2021-pecert

Centro Nacional de Seguridad Digital. *Alerta integrada de seguridad digital* N.º 108-2021. Lima: 6 de mayo de 2021. https://www.gob.pe/institucion/pcm/informes-publicaciones/1896577-alerta-integrada-de-seguridad-digital-n-108-2021-pecert

Centro Nacional de Seguridad Digital. *Alerta integrada de seguridad digital* N.º 161-2021. Lima: 1 de julio de 2021. https://www.gob.pe/institucion/pcm/informes-publicaciones/2002739-alerta-integrada-de-seguridad-digital-n-161-2021-pecert

Centro Nacional de Seguridad Digital. *Alerta integrada de seguridad digital* N.º 65-2022. Lima: 6 de marzo de 2022. https://www.gob.pe/institucion/pcm/informes-publicaciones/2798506-alerta-integrada-de-seguridad-digital-n-065-2022-cnsd

Centro Nacional de Seguridad Digital. *Alerta integrada de seguridad digital* N.º 260-2022. Lima: 23 de setiembre de 2022. https://www.gob.pe/institucion/pcm/informes-publicaciones/3522084-alerta-integrada-de-seguridad-digital-n-260-2022-cnsd

Centro Nacional de Seguridad Digital. *Alerta integrada de seguridad digital* N.º 294-2023. Lima: 11 de diciembre del 2023. https://cdn.www.gob.pe/uploads/document/file/5550553/4934553-alerta-integrada-de-seguridad-digital-n-294-2023-cnsd.pdf

Centro Nacional de Seguridad Digital. *Alerta integrada de seguridad digital* N.º 64-2024. Lima: 14 de marzo de 2024. https://www.gob.pe/institucion/pcm/informes-publicaciones/5367163-alerta-integrada-de-seguridad-digital-n-064-2024-cnsd

Centro Nacional de Seguridad Digital. *Alerta integrada de seguridad digital* N.º 148-2024. Lima: 26 de junio de 2024. https://www.gob.pe/institucion/pcm/informes-publicaciones/5702366-alerta-integrada-de-seguridad-digital-n-148-2024-cnsd

Centro Nacional de Seguridad Digital. *Alerta integrada de seguridad digital* N.º 162-2024. Lima: 12 de julio de 2024. https://www.gob.pe/institucion/pcm/informes-publicaciones/5776792-alerta-integrada-de-seguridad-digital-n-162-2024-cnsd

Centro Nacional de Seguridad Digital. *Alerta integrada de seguridad digital* N.º 164-2024. Lima: 15 de julio de 2024. https://www.gob.pe/institucion/pcm/informes-publicaciones/5785248-alerta-integrada-de-seguridad-digital-n-164-2024-cnsd

Centro Nacional de Seguridad Digital. *Alerta integrada de seguridad digital* N.º 255-2024. Lima: 5 de noviembre de 2024. https://www.gob.pe/institucion/pcm/informes-publicaciones/6150042-alerta-integrada-de-seguridad-digital-n-255-2024-cnsd

Centro Nacional de Seguridad Digital. *Alerta integrada de seguridad digital* N.º 260-2024. Lima: 11 de noviembre de 2024. https://www.gob.pe/institucion/pcm/informes-publicaciones/6169391-alerta-integrada-de-seguridad-digital-n-260-2024-cnsd

Centro Nacional de Seguridad Digital. *Alerta integrada de seguridad digital* N.º 261-2024. Lima: 12 de noviembre de 2024. https://www.gob.pe/institucion/pcm/informes-publicaciones/6174849-alerta-integrada-de-seguridad-digital-n-261-2024-cnsd

Centro Nacional de Seguridad Digital. *Alerta integrada de seguridad digital* N.º 262-2024. Lima: 13 de noviembre de 2024. https://www.gob.pe/institucion/pcm/informes-publicaciones/6183321-alerta-integrada-de-seguridad-digital-n-262-2024-cnsd

Centro Nacional de Seguridad Digital. *Alerta integrada de seguridad digital* N.º 273-2024. Lima: 26 de noviembre de 2024. https://www.gob.pe/institucion/pcm/informes-publicaciones/6232419-alerta-integrada-de-seguridad-digital-n-273-2024-cnsd

Centro Nacional de Seguridad Digital. *Alerta integrada de seguridad digital* N.º 274-2024. Lima: 27 de noviembre de 2024. https://www.gob.pe/institucion/pcm/informes-publicaciones/6240167-alerta-integrada-de-seguridad-digital-n-274-2024-cnsd

Centro Nacional de Seguridad Digital. *Alerta integrada de seguridad digital* N.º 275-2024. Lima: 28 de noviembre de 2024. https://www.gob.pe/institucion/pcm/informes-publicaciones/6247921-alerta-integrada-de-seguridad-digital-n-275-2024-cnsd

Congreso de la República. *Diario de los debates*. Sesión del 21 de junio de 2000.

Council of Europe. *Computer-related crime. Recommendation N.º R (89) 9 on computer-related crime and final report of the European Committee on Crime Problems*. Strasbourg, 1990.

Council of Europe. *Convenio sobre la ciberdelincuencia*, Budapest, 23 de noviembre de 2001. https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Council of Europe. *Convenio sobre la ciberdelincuencia. Informe explicativo*, Budapest, 23 de noviembre de 2001. https://rm.coe.int/16802fa403

Council of Europe. *The global state of cybercrime legislation 2013-2024: A cursored overview*, 2025. https://rm.coe.int/3148-1-3-4-cyberleg-global-state-dec-2024-public-v6-final/1680b3ecc5

Crawley, Kim. *Cultura hacker de la A a la Z. Una guía divertida de las personas, ideas y artefactos que han construido el mundo de la tecnología*. Madrid: Ediciones Anaya Multimedia, 2024.

Drug Enforcement Administration. *National Drug Threat Assessment 2024*. https://www.dea.gov/sites/default/files/2024-07/2024%20NDTA-updated%207.5.2024.pdf

Dudinskikh, Karina. *La botnet Matrix desata ataques DDoS masivos explotando dispositivos IoT vulnerables*, en *UAD*, 27 de noviembre de 2024. https://unaaldia.hispasec.com/2024/11/la-botnet-matrix-desata-ataques-ddos-masivos-explotando-dispositivos-iot-vulnerables.html

Elías Puelles, Ricardo. *Decreto Legislativo 1182. Geolocalización y proceso penal. Sacrificios de garantías en favor de una supuesta eficacia investigativa*. Lima: Hiperderecho, 2016. https://hiperderecho.org/wp-content/uploads/2016/05/elias_geolocalizacion_proceso_penal.pdf

European Union Agency For Law Enforcement Cooperation. *Internet Organised Crime Threat Assessment (IOCTA) 2024*. Luxemburgo: Publications Office of the European Union, 2024. https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024

Fernández-Cruz, Francisco José y María José Fernández Díaz. "Los docentes de la Generación Z y sus competencias digitales". En: *Comunicar. Revista Científica de Comunicación y Educación* N.º 46, 2016. https://www.revistacomunicar.com/index.php?contenido=detalles&numero=46&articulo=46-2016-10

Gómez Vieites, Álvaro. *Enciclopedia de la Seguridad Informática*. Madrid: RA-MA Editorial y Publicaciones. [Kindle]

González Bello, Edgar Oswaldo y Adolfo Castillo Navarro. "La enseñanza universitaria en derecho con el uso didáctico de las TIC". En: *Dike, Revista de Investigación en Derecho y Criminología*, 2016. http://www.apps.buap.mx/ojs3/index.php/dike/article/view/235

Informe del Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente. Viena, 10 al 17 de abril de 2000. https://www.unodc.org/documents/congress/Previous_Congresses/10th_Congress_2000/030_ACONF.187.15_Report_of_the_Tenth_United_Nations_Congress_on_the_Prevention_of_Crime_and_the_Treatment_of_Offenders_S.pdf Internet Crime Complaint Center. *Federal Bureau*

of Investigation: Internet Crime Report 2023. https://www.aha.org/system/files/media/file/2024/03/fbi-internet-crime-report-2023.pdf

Instituto Nacional de Ciberseguridad [España]. *Bloqueo de dispositivos: patrón, contraseña, PIN, código y biometría*. https://www.incibe.es/ciudadania/tematicas/dispositivos-moviles/bloqueo-dispositivos

Instituto Nacional de Ciberseguridad [España]. *¿Cómo manejar una brecha de seguridad. Pasos críticos: desde la contención hasta la recuperación y comunicación con los afectados?* https://www.incibe.es/sites/default/files/Emprendimiento/Guía_manejar_brecha_seguridad/Guía_Cómo%20manejar%20una%20brecha%20de%20seguridad.pdf

Instituto Nacional de Ciberseguridad [España]. *Con estos ataques nos roban las contraseñas, ¡aprende a evitarlos!* https://www.incibe.es/empresas/blog/estos-ataques-nos-roban-las-contrasenas-aprende-evitarlos

Instituto Nacional de Ciberseguridad [España]. *Keylogger*. https://www.incibe.es/node/494000

Instituto Nacional de Ciberseguridad [España]. *Protección de la información*. https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_proteccion-de-la-informacion.pdf

Instituto Nacional de Estadística e Informática. Informe Técnico N.º 02 – Junio de 2024, *Estadística de las Tecnologías de Información y Comunicación en los Hogares. Trimestre: Enero-Febrero-Marzo 2024*. https://cdn.www.gob.pe/uploads/document/file/6543264/5702640-las-tecnologias-de-informacion-y-comunicacion-en-los-hogares-ene-feb-mar-2024.pdf

Jacoby, David. "El mercado negro de los certificados académicos", en *Kaspersky Daily*, 24 de julio de 2019. https://www.kaspersky.es/blog/school-hacking/18736/?srsltid=AfmBOop4hGsJAbqd-J8MK_JqLfRUZa-A3Bh3wXeygi1qF_MiqKSh9-G9

Kiner, Emil y Tim April, "Google mitigated the largest DDoS attack to date, peaking above 398 million rps", en *Google cloud*. 10 de octubre de 2023. https://cloud.google.com/blog/products/identity-security/google-cloud-mitigated-largest-ddos-attack-peaking-above-398-million-rps

López Rubio, Daniel. "Twitter: Una herramienta auxiliar en la docencia del derecho constitucional". En: *Docencia y Derecho. Revista para la docencia jurídica universitaria* 15, 2020. https://www.uco.es/docencia_derecho/index.php/reduca/article/viewFile/201/253

Lucich, John. *Pocket guide for investigating ransomware and network intrusions.* StarPath Publications, 2021. [Kindle]

Marion, Nancy E. y Jason Twede. *Cybercrime. An Encyclopedia of Digital Crime.* California: ABC-Clio, 2020. [Kindle]

Mayer Lux, Laura. "El bien jurídico protegido en los delitos informáticos". En: *Revista Chilena de Derecho.* Vol. 44. N.° 1. Santiago: 2017. https://www.scielo.cl/pdf/rchilder/v44n1/art11.pdf

Ministerio De Justicia y Derechos Humanos. *Ciberdelincuencia. Reporte de información estadística y recomendaciones para la prevención,* 2022. https://cdn.www.gob.pe/uploads/document/file/3562747/Reporte%20de%20Ciberdelincuencia.pdf.pdf

Miguel Román, José Antonio. "La educación superior en tiempos de pandemia: Una visión desde dentro del proceso formativo". En: *Revista Latinoamericana de Estudios Educativos,* vol. L, número especial, México: 2020. https://www.redalyc.org/jatsRepo/270/27063237017/html/index.html

Miranda, Elena, "Cómo ciberdelincuentes vulneraron seguridad del INDECI y propagaron virus con reportes de lluvias", en *Convoca,* Lima 18 de marzo de 2023. https://convoca.pe/agenda-propia/como-ciberdelincuentes-vulneraron-seguridad-del-indeci-y-propagaron-virus-con

Observatorio de criminalidad del Ministerio Público. "Delitos informáticos registrados por el Ministerio Público. Enero 2000 – Diciembre 2010". En: *Persecución estratégica del delito.* Año 2. N.° 2, febrero. Lima: Ministerio Público, 2011.

Octavo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente. La Habana, 27 de agosto a 7 de setiembre de 1990. https://www.unodc.org/documents/congress/Previous_Congresses/8th_Congress_1990/028_ACONF.144.28.Rev.1_Report_Eighth_United_Nations_Congress_on_the_Prevention_of_Crime_and_the_Treatment_of_Offenders_S.pdf

Organización de los Estados Americanos. *Conclusiones y recomendaciones (Adoptadas en la quinta sesión de trabajo celebrada el 3 de diciembre de 1997).* Reunión de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas. 1 al 3 de diciembre de 1997. Buenos Aires, 1997. https://www.oas.org/juridico/spanish/remjai_recomend.pdf

Organización de los Estados Americanos. *Informe Final de la Segunda Reunión de Ministros de Justicia o de Ministros Procuradores Generales de las Américas.* 1999. https://www.oas.org/juridico/spanish/remjaii_inf_final.pdf

Organización de los Estados Americanos. *Informe Final de la Tercera Reunión de Ministros de Justicia o de Ministros Procuradores Generales de las Américas.* 2000. https://www.oas.org/consejo/sp/grupostrabajo/docs/mj00177s04.doc

Organización de los Estados Americanos. *Informe Final de la Cuarta Reunión de Ministros de Justicia o de Ministros Procuradores Generales de las Américas.* 2002. https://www.oas.org/juridico/spanish/remjaiv_inf_final.pdf

Organización de los Estados Americanos. *Informe Final de la Quinta Reunión de Ministros de Justicia o de Ministros Procuradores Generales de las Américas.* 2004. https://www.oas.org/juridico/spanish/remjaV_inf_final.pdf

Organización de los Estados Americanos. *Informe Final de la Sexta Reunión de Ministros de Justicia o de Ministros Procuradores Generales de las Américas.* 2006.

Organización de los Estados Americanos. *Conclusiones y recomendaciones (Aprobadas en la quinta plenaria el 26 de abril de 2006 y revisada por la Comisión de Estilo en las sesiones celebradas los días 19 y 21 de julio y 3 de agosto de 2006).*

Organización de los Estados Americanos. *Conclusiones y recomendaciones de la REMJA VII.* 2008. https://www.oas.org/juridico/spanish/cybVII_CR.pdf

Organización de los Estados Americanos. *Conclusiones y recomendaciones de la REMJA VIII.* 2010. https://www.oas.org/dil/esp/REMJA-VIII_doc_4-10_rev1_esp.doc

Organización de los Estados Americanos. *Conclusiones y recomendaciones de la REMJA IX.* 2012. https://cejamericas.org/wp-content/uploads/2019/12/REMJA_IX-1.pdf

Organización de los Estados Americanos. *Conclusiones y recomendaciones de la REMJA X.* 2015. https://www.oas.org/es/sla/dlc/remja/pdf/remja_x_rec_conc_sp.pdf

Organización de los Estados Americanos. *Conclusiones y recomendaciones de la REMJA XI.* 2021. https://www.oas.org/es/sla/dlc/remja/pdf/remja_xi_rec_conc_sp.pdf

Poder Judicial de la nación de Argentina. *Ciberdelitos y evidencia digital.* Secretaria de Jurisprudencia. 2024. https://mendozalegal.com/omeka/files/original/99099382dd28a7301f9bb5a885626b1a.pdf

Programa de las Naciones Unidas para el Desarrollo. *Informe sobre Desarrollo Humano en Venezuela 2002. Las tecnologías de la información y la comunicación al servicio del desarrollo.* https://hdr.undp.org/system/files/documents/venezuela2002es.pdf

Root, Enoch, "ILOVEYOU: el virus que amaba a todo el mundo", en *Kaspersky Daily*, 11 de agosto de 2022. https://www.kaspersky.es/blog/cybersecurity-history-iloveyou/27485/

Tanata Vásquez, Heydi. "Educación superior en tiempos de pandemia". En: *Ciencia Latina Revista Científica Multidisciplinar 5(6)*, México: 2021. https://ciencialatina.org/index.php/cienciala/article/view/1368/1886

C. LEGISLACIÓN Y OTROS DOCUMENTOS LEGALES

Consejo de Europa. *Convenio sobre la Ciberdelincuencia.* Budapest: 23 de noviembre de 2001.

Consejo de Europa. *Informe Explicativo del Convenio sobre la Ciberdelincuencia*, 2001

Congreso de la república del Perú. *Código Penal, Decreto Legislativo 635.* Lima: 8 de abril de 1991.

Congreso de la república del Perú. *Ley N.º 30 096, Ley de Delitos Informáticos*. Lima: 22 de octubre de 2013.

Congreso de la república del Perú. *Ley N.º 30171, Ley que modifica la Ley N.º 30 096, Ley de Delitos Informáticos*. Lima: 10 de marzo de 2014.

Congreso de la república del Perú. *Proyecto de Ley N.º 5 071/99-CR, proyecto de ley de delitos informáticos*. Presentado el 18 de agosto de 1999.

Congreso de la república del Perú. *Proyecto de Ley N.º 5 132/99-CR, proyecto de ley que propone establecer como figura típica penal los delitos informáticos*. Presentado el 31 de agosto de 1999.

Congreso de la república del Perú. *Proyecto de Ley N.º 5 326/99-CR*. Presentado el 18 de octubre de 1999.

Congreso de la república del Perú. *Proyecto de Ley N.º 1 744, proyecto de ley que modifica los art. 207-A, 207-B y 207-C del Título V del Libro II del Código Penal, DL 635 referente a los delitos informáticos*. Presentado el 20 de abril de 2001.

Congreso de la república del Perú. *Proyecto de Ley N.º 2 226/2003-CR*. Presentado el 12 de marzo de 2002.

Congreso de la república del Perú. *Proyecto de Ley N.º 7 197, proyecto de ley que incorpora el artículo 207-D al Código Penal sobre los delitos informáticos*. Presentado el 13 de junio de 2003.

Congreso de la república del Perú. *Proyecto de Ley N.º 7 807/2003-CR, proyecto de ley de delitos informáticos, estafa y fraudes*. Presentado el 12 de agosto de 2003.

Congreso de la república del Perú. *Proyecto de Ley N.º 10 079/2003-CR, proyecto de ley que modifica el art. 207-B y agrega al Capítulo X Delitos Informáticos del Título V del Código Penal, los artículos 207-D, 207-E, 207-F y 207-G*. Presentado el 17 de marzo de 2004.

Congreso de la república del Perú. *Proyecto de Ley N.º 11 346/2004-CR, proyecto de ley que incorpora nuevas figuras delictivas al Código de Justicia Militar*. Presentado el 6 de setiembre de 2004.

Congreso de la república del Perú. *Proyecto de Ley N.º 11 402/2004-CR, proyecto de ley que modifica el artículo 207-A del Código Penal referido a los delitos informáticos*. Presentado el 10 de setiembre de 2004.

Congreso de la república del Perú. *Proyecto de Ley N.º 1 318/2006-CR, proyecto de ley de represión de los delitos informáticos*. Presentado el 21 de mayo de 2007.

Congreso de la república del Perú. *Proyecto de Ley N.º 1 828/2007-CR, proyecto de ley que penaliza los delitos informáticos*. Presentado el 31 de octubre de 2007.

Congreso de la república del Perú. *Proyecto de Ley N.º 3 083/2008-CR, proyecto de ley que regula los delitos informáticos*. Presentado el 12 de marzo de 2009.

Congreso de la república del Perú. *Proyecto de Ley N.º 4 279/2010-CR, proyecto de ley que propone crear un sistema regulador y sancionador respecto al uso de las Tecnologías de la Información y Comunicaciones (TIC)*. Presentado el 2 de setiembre de 2010.

Congreso de la república del Perú. *Proyecto de Ley N.º 34/2011-CR, proyecto de ley que regula los delitos informáticos*. Presentado el 11 de agosto de 2011.

Congreso de la república del Perú. *Proyecto de Ley N.º 307/2011-CR, proyecto de ley especial sobre delitos cometidos con el uso de las Tecnologías de la Información y Comunicación*. Presentado el 5 de octubre de 2011.

Congreso de la república del Perú. *Proyecto de Ley N.º 1 136/2011-CR, proyecto de ley que modifica el artículo 207-C del Código Penal, incorporando el delito de robo de identidad virtual e incorpora el artículo 207-D – delito informático agravado*. Presentado el 17 de mayo de 2012.

Congreso de la república del Perú. *Proyecto de Ley N.º 1 257/2011-CR, proyecto de ley que agrava los delitos de violación del secreto de las comunicaciones*. Presentado el 14 de junio de 2012.

Congreso de la república del Perú. *Proyecto de Ley N.º 2 112/2012-CR, proyecto de ley que modifica e incorpora diversos artículos al Código Penal sobre el uso ilegal de servicios de telecomunicaciones*. Presentado el 12 de abril de 2013.

Congreso de la república del Perú. *Proyecto de Ley N.º 2 129/2012-CR, proyecto de ley que sanciona la venta ilegal de base de datos y datos personales de usuarios y consumidores.* Presentado el 16 de abril de 2013.

Congreso de la república del Perú. *Proyecto de Ley N.º 2 398/2012-CR, proyecto de ley que modifica el artículo 176 del Código Penal e incorpora el artículo 176-B, el delito de utilización de los medios electrónicos, telefónicos u otras tecnologías de transmisión de datos para ejercer influencias contra un menor para actividades sexuales explícitas o actos con connotación sexual.* Presentado el 1 de julio de 2013.

Congreso de la república del Perú. *Proyecto de Ley N.º 2 482/2012-CR, proyecto de ley que incorpora el artículo 173-A en el Código Penal tipificando el delito de acoso sexual infantil mediante nuevas tecnologías de información y telecomunicaciones.* Presentado el 17 de julio de 2013.

Congreso de la república del Perú. *Proyecto de Ley N.º 2 520/2012-PE, proyecto de ley de represión de la cibercriminalidad.* Presentado el 26 de julio de 2013.

Congreso de la república del Perú. *Proyecto de Ley N.º 2 991/2013-CR, proyecto de ley que modifica la ley 30 096, Ley de Delitos Informáticos.* Presentado el 25 de noviembre del 2013.

Congreso de la república del Perú. *Proyecto de Ley N.º 2 999/2013-CR, proyecto de ley que modifica, incorpora y deroga diversos artículos a la ley 30096, Ley de Delitos Informáticos.* Presentado el 27 de noviembre de 2013.

Congreso de la república del Perú. *Proyecto de Ley N.º 3 017/2013-CR, proyecto de ley que modifica la ley 30 096, Ley de Delitos Informáticos.* Presentado el 29 de noviembre de 2013.

Congreso de la república del Perú. *Proyecto de Ley N.º 3 048/2013-CR, proyecto de ley que modifica la ley 30 096, Ley de Delitos Informáticos.* Presentado el 5 de diciembre de 2013.

Congreso de la república del Perú. *Proyecto de Ley N.º 3 105/2013-CR, proyecto de ley que modifica la Ley N.º 30 096, Ley de Delitos Informáticos.* Presentado el 18 de diciembre de 2013.

Congreso de la república del Perú. *Proyecto de Ley N.º 3 980/2014-CR, Proyecto de ley que propone modificar la Ley N.º 30096, Ley de Delitos Informáticos, modificada por la Ley N.º 30171.* Presentado el 13 de noviembre de 2014.

Congreso de la república del Perú. *Proyecto de Ley N.º 1 037/2016-CR, proyecto de ley que declara la imprescriptibilidad de los delitos de violación de la libertad sexual e incrementa sus penas.* Presentado el 8 de marzo de 2017.

Congreso de la república del Perú. *Proyecto de Ley N.º 3 427/2018-CR, proyecto de ley que incorpora el delito de acoso virtual o ciberacoso en la Ley N.º 30 096, Ley de Delitos Informáticos.* Presentado el 24 de setiembre de 2018.

Congreso de la república del Perú. *Proyecto de Ley N.º 4 643/2019-CR, proyecto de ley que declara de interés nacional y necesidad pública la creación de la Fiscalía Especializada en Delitos Informáticos.* Presentado el 2 de agosto de 2019.

Congreso de la república del Perú. *Proyecto de Ley N.º 5 226/2020-CR, proyecto de ley que penaliza como forma agravada los delitos de hurto, robo y estafa y los delitos informáticos cometidos durante un estado de emergencia nacional.* Presentado el 15 de mayo de 2020.

Congreso de la república del Perú. *Proyecto de Ley N.º 5 630/2020-CR, proyecto de ley de seguridad informática y represión de los delitos informáticos.* Presentado el 25 de junio de 2020.

Council of Europe. *Computer-related crime. Recommendation N.º R (89) 9 on computer-related crime and final report of the European Committee on Crime Problems.* Strasbourg, 1990.

Ministerio Público del Perú. *Resolución de la Fiscalía de la Nación N.º 1503-2020-MP-FN, Crean la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público con competencia nacional y designan y nombran Fiscales en el Distrito Fiscal de Lima.* Lima: 30 de diciembre del 2020.

Ministerio Público del Perú. *Resolución de la Junta de Fiscales Supremos N.º 061-2023-MP-FN-JFS.* Lima: 12 de agosto del 2023

Poder Ejecutivo. *Decreto Legislativo N.º 1182.* Lima: 27 de julio del 2015

Poder Ejecutivo. *Decreto Supremo N.º 010-2019-RE, Ratifican el Convenio sobre la Ciberdelincuencia*. Lima: 10 de marzo de 2019.

Poder Ejecutivo. *Decreto Legislativo N.º 1614, Decreto Legislativo que modifica la Ley N.º 30096, Ley de Delitos Informáticos, para prevenir y hacer frente a la delincuencia*. Lima: 21 de diciembre del 2023.

D. FUENTES JURISPRUDENCIALES

D.1 España

- SAN 704/2016. Sentencia N.º 14/16 del 3 de marzo de 2016, emitida por el Juzgado de Instrucción N.º 3 de la Audiencia Nacional. Sala de lo Penal de Madrid. Ponente: Carmen González Pastor.
- SAN 6038/2023. Sentencia N.º 21/2023 del 30 de noviembre del 2023, emitida por la Sala de lo Penal de la Audiencia Nacional de España, Sección N.º 1. Ponente: Jesús Eduardo Gutiérrez Gómez.
- SAN 48/2024. Sentencia N.º 1/2024 del 9 de enero del 2024, emitida por la Sala de lo Penal de la Audiencia Nacional de Madrid, Sección N.º 1. Ponente: Adoración María Riera Ocariz.
- SAN 1712/2024. Sentencia N.º 39/2023 del 6 de setiembre del 2023, emitida por la Audiencia Provincial de Melilla, Sección N.º 7. Ponente: Aaron Andueza Jiménez.
- SAN 1712/2024. Sentencia N.º 7/2024 del 5 de abril de 2024, emitida por la Sala Penal de la Audiencia Nacional de Madrid, Sección N.º 3. Ponente: Ana María Rubio Encinas.
- SAP 623/2003. Sentencia N.º 127/2003 del 4 de abril de 2003, emitida por la Audiencia Provincial de Tarragona, Sección N.º 2. Ponente: Xavier Nouvilas Puig.
- SAP 8452/2015. Sentencia N.º 37/2015 del 11 de junio de 2015, emitida por la Audiencia Provincial de Madrid, Sección N.º 30. Ponente: María Pilar Olivan Lacasta.

- SAP 636/2016. Sentencia N.º 205/2016 del 29 de junio de 2016, emitida por la Audiencia Provincial de Valladolid, Sección N.º 4. Ponente: Ángel Santiago Martínez García.
- SAP VA 440/2020. Sentencia N.º 82/2020 del 8 de junio de 2020, emitida por la Audiencia Provincial de Valladolid, Sección N.º 2. Ponente: Juan Miguel Donis Carracedo.
- SAP 2072/2021. Sentencia N.º 189/2021 del 12 de mayo de 2021, emitida por la Audiencia Provincial de Málaga, Sección N.º 3. Ponente: Juan Carlos Hernández Oliveros.
- SAP 2160/2022. Sentencia N.º 345/2022 del 28 de setiembre de 2022, emitida por la Audiencia Provincial de Vigo, Sección N.º 5. Ponente: José Ramón Sánchez Herrero.
- SAP 1105/2023. Sentencia N.º 203/2023 del 12 de junio de 2023, emitida por la Audiencia Provincial de Zaragoza, Sección N.º 3. Ponente: Nicolasa García Roncero.
- SAP 78/2024. Sentencia N.º 35/2024 del 26 de enero de 2024, emitida por la Audiencia Provincial de Zaragoza, Sección N.º 6. Ponente: Francisco José Picazo Blasco.
- SAP 314/2024. Sentencia N.º 89/2024 del 22 de marzo de 2024, emitida por la Audiencia Provincial de Ciudad Real, Sección N.º 2. Ponente: María Almudena Buzón Cervantes.
- SAP 430/2024. Sentencia N.º 155/2024 del 17 de julio de 2024, emitida por la Audiencia Provincial de Ourense, Sección N.º 2. Ponente: María de los Ángeles Lamas Méndez.
- SAP 7446/2024. Sentencia N.º 288/2024 del 17 de mayo de 2024, emitida por la Audiencia Provincial de Madrid, Sección N.º 9. Ponente: Juana de la Cruz Serrano Gonzáles.
- SAP CC 1127/2011. Sentencia N.º 276/2021 del 26 de octubre del 2021, emitida por la Audiencia Provincial de Cáceres, Sección N.º 2. Ponente: Julia Domínguez Domínguez.

- SAP LE 528/2021. Sentencia N.º 94/2021 del 4 de marzo de 2021, emitida por la Audiencia Provincial de León, Sección N.º 3. Ponente: María del Mar Gutiérrez Puente.
- SAP LE 560/2024. Sentencia N.º 127/2024 del 26 de marzo del 2024, emitida por la Audiencia Provincial de León, Sección N.º 3. Ponente: Nuria Valladares Fernández.
- SJP 48/2014. Sentencia N.º 238/2014 del 24 de junio de 2014, emitida por el Juzgado de lo Penal de Alcalá de Henares, Sección N.º 4. Ponente: Nuria Alcalde Alcalde.
- SJP 36/2020. Sentencia N.º 267/2020 del 24 de setiembre 2020, emitida por el Juzgado de Valencia, Sección N.º 12. Ponente: Margarita Sierra Serrano.
- SJP 31/2022. Sentencia N.º 499/2022 del 23 de diciembre de 2022, emitida por el Juzgado de lo Penal de Valencia, Sección N.º 6. Ponente: Begoña Estañ Capell.
- STS 1008/2024. Sentencia N.º 183/2024 del 29 de febrero del 2024, emitida por la Sala de lo Penal del Tribunal Supremo de España, Sección N.º 1. Ponente: Carmen Lamela Díaz.
- STS 3040/2018. Sentencia N.º 377/2018 del 23 de julio de 2018, emitida por la Sala de lo Penal de Madrid del Tribunal Supremo, Sección N.º 1. Ponente: Vicente Magro Servet.
- STS 469/2022. Sentencia N.º 42/2021 del 18 de enero del 2022, emitida por la Sala de lo Civil y Penal del Tribunal Superior de Justicia de Palma de Mallorca, Sección N.º 1. Ponente: Antonio Federico Capo Delgado.
- STS 2897/2024. Sentencia N.º 476/2024 del 22 de mayo de 2024, emitida por la Sala de lo Penal del Tribunal Supremo, Sede Madrid. Ponente: Manuel Marchena Gómez.
- STSJ 1673/2023. Sentencia N.º 00062/2023 del 14 de diciembre de 2023, emitida por el Tribunal Superior de Justicia de lo Civil y Penal de Palma de Mallorca, Sección N.º 1. Ponente: Diego Jesús Gómez-Reino Delgado.

D.2. Perú

Poder Judicial Del Perú

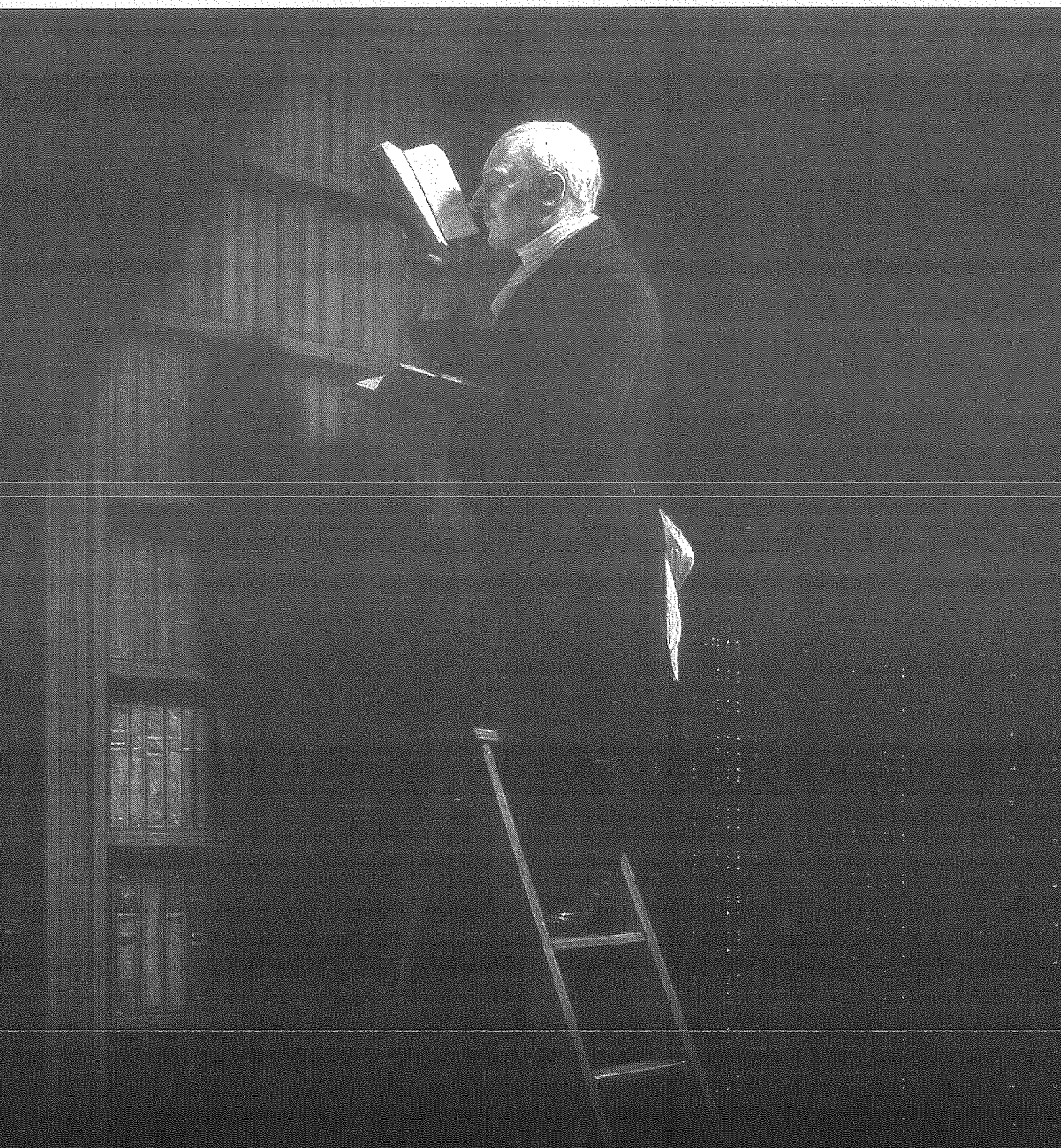
- Casación N.º 305-2021, Lambayeque del 23 de junio del 2022, emitida por la Sala Penal Permanente de la Corte Suprema de Justicia de la República del Perú.
- Casación N.º 453-2022, Nacional del 4 de noviembre del 2024, emitida por la Sala Penal Permanente de la Corte Suprema de Justicia de la República del Perú.
- Casación N.º 3330-2022, El Santa del 14 de febrero de 2024, emitida por la Sala Penal Permanente de la Corte Suprema de Justicia de la República del Perú.
- R. N. N.º 2932-2016, Lima del 12 de junio del 2017, emitida por la Primera Sala Penal Transitoria de la Corte Suprema de Justicia de la República del Perú.
- R. N. N.º 743-2018, Lima del 26 de octubre de 2018, emitida por la Sala Penal Permanente de la Corte Suprema de Justicia de la República del Perú.
- R. N. N.º 805-2018, Lima del 11 de abril de 2019, emitida por la Sala Penal Transitoria de la Corte Suprema de Justicia de la República del Perú.
- R. N. N.º 760-2020, Lima del 5 de abril del 2021, emitida por la Sala Penal Permanente de la Corte Suprema de Justicia de la República del Perú.
- R. N. N.º 557-2024, Lima del 27 de agosto de 2024, emitida por la Sala Penal Transitoria de la Corte Suprema de Justicia de la República del Perú.

Tribunal Constitucional del Perú

- Sentencia recaída sobre el Exp. N.º 006-2014-PI/TC. Lima: 5 de marzo del 2020.
- Sentencia recaída sobre el Exp. N.º 019-2005-PI/TC. Lima: 21 de julio del 2005.

- Sentencia recaída sobre el Exp. N.º 5994-2005-PHC/TC: Lima: 29 de agosto del 2005
- Sentencia recaída sobre el Exp. N.º 04094-2011-PA/TC. Lima: 23 de enero del 2012.

ÍNDICES



* La ilustración de la página anterior corresponde a una adaptación de "El ratón de la biblioteca" de Carl Spitzweig (1850). Para su elaboración se empleó OpenAI.

Sumario: I. Índice de casos. II. Índice de cuadros. III. Índice de diagramas. IV. Índice de esquemas e imágenes.

I. ÍNDICE GENERAL

Agradecimientos 9
Prólogo 11
Presentación 17
Abreviaturas 21
Introducción 25

CAPÍTULO 1
LA CIBERDELINCUENCIA COMO UN FENÓMENO GLOBAL

1.1. Introducción 42
1.2. De internet a la sociedad de la información 42
1.3. El impacto global de las tecnologías de la información y la comunicación 47
1.3.1. Las tecnologías de la información y la comunicación 47
1.3.2. El impacto positivo de las TIC 50
1.3.2.1. A nivel industrial 51
1.3.2.2. A nivel social 53
1.3.2.3. A nivel educativo 55
1.3.2.4. A nivel judicial 59
1.3.3. El impacto negativo de las TIC: facilitan la comisión de delitos y crean otros tantos 61
1.4. Ciberataques puros, réplica y de contenido 66
1.4.1. Ciberataques puros 67
1.4.1.1. *Hacking* 67
1.4.1.2. *Malware* intrusivo 68
1.4.1.3. *Malware* destructivo 69
1.4.1.4. Ataques de *insiders* 69
1.4.1.5. Ataques DoS 70
1.4.1.6. *Spam* 71
1.4.1.7. Ciberocupación 72
1.4.1.8. *Antisocial networks* 72

1.4.1.9. Ciberguerra o *cyberwar* 73
1.4.1.10. Ciberactivismo o *cyberhacktivism* 73
1.4.2. Ciberataques réplica 75
1.4.2.1. Ciberfraudes 75
1.4.2.2. *Phishing* 76
1.4.2.3. *Pharming* 77
1.4.2.4. *Scam* 78
1.4.2.5. *Auction fraud* 79
1.4.2.6. *Cyberspyware* 79
1.4.2.7. Uso de *sniffers* 80
1.4.2.8. Ciberespionaje de empresas 81
1.4.2.9. *Identity theft* 82
1.4.2.10. *Spoofing* 84
1.4.2.11. *DNS spoofing* 85
1.4.2.12. *ARP spoofing* 85
1.4.2.13. *IP spoofing* 86
1.4.2.14. *Web spoofing* 87
1.4.2.15. Ciberblanqueo de capitales 88
1.4.2.16. Ciberextorsión 89
1.4.2.17. Ciberocupación 91
1.4.2.18. *Cyberstalking* 91
1.4.2.19. *Cyberbullying* 92
1.4.2.20. *Online harassment* 93
1.4.2.21. *Sexting* 94
1.4.2.22. Extorsión con imágenes de *sexting* 95
1.4.2.23. *Online grooming* 95
1.4.2.24. Ciberespionaje terrorista 96
1.4.3. Ciberataques de contenido 97
1.4.3.1. Distribución de pornografía infantil en internet 97
1.4.3.2. Ciberpiratería intelectual 98
1.4.3.3. *Online hate speech* 99
1.4.3.4. Ciberterrorismo 100
1.5. Conclusiones del capítulo 102

CAPÍTULO 2
LA LUCHA INTERNACIONAL CONTRA LA CIBERCRIMINALIDAD

2.1. Introducción 108
2.2. Estudios y esfuerzos iniciales 110
2.3. Estados pioneros que incorporaron los delitos informáticos en la legislación local 113
2.4. Sistema europeo 117
2.4.1. Conferencia sobre aspectos criminológicos de los delitos económicos, 1976 117

2.4.2. Convenio N.º 108 del Consejo de Europa, para la protección de personas con respecto al tratamiento informatizado de datos personales, 1981.. 118
2.4.3. Recomendaciones de la OCDE, 1986 118
2.4.4. Recomendaciones del Consejo de Europa, 1989 119
2.4.5. Recomendaciones del Consejo de Europa, 1995 122
2.4.6. Protocolo adicional al Convenio N.º 108, relativo a autoridades de supervisión y flujos internacionales de datos, 2001 123
2.4.7. Convenio sobre la Ciberdelincuencia, 2001 123
2.4.8. Primer Protocolo adicional al Convenio sobre Ciberdelincuencia, relativo a la penalización de actos de naturaleza racista y xenófoba cometidos por medio de sistemas informáticos, 2003 129
2.4.9. Convenio del Consejo de Europa para la protección de los niños contra la explotación y el abuso sexual, 2007 130
2.4.10. Directiva 2016/680 del Parlamento Europeo y del Consejo de Europa, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales y la libre circulación de dichos datos, 2016 131
2.4.11. Segundo Protocolo adicional al Convenio sobre la Ciberdelincuencia, relativo a la cooperación reforzada y la divulgación de prueba electrónica, 2022 132
2.5. Sistema interamericano 133
2.5.1. Segunda Reunión de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas sobre Delito Cibernético, 1999 133
2.5.2. Tercera Reunión de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas sobre Delito Cibernético, 2000 135
2.5.3. Cuarta Reunión de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas sobre Delito Cibernético, 2002 136
2.5.4. Quinta Reunión de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas sobre Delito Cibernético, 2004 137
2.5.5. Estrategia Interamericana Integral para Combatir las Amenazas a la Seguridad Cibernética: un enfoque multidimensional y multidisciplinario para la creación de una cultura de seguridad cibernética, 2004 138
2.5.6. Sexta Reunión de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas sobre Delito Cibernético, 2006 139
2.5.7. Séptima Reunión de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas sobre Delito Cibernético, 2008 141
2.5.8. Octava Reunión de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas sobre Delito Cibernético, 2010 141
2.5.9. Declaración de Río sobre el Delito Cibernético, 2012 142
2.5.10. Novena Reunión de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas sobre Delito Cibernético, 2012 143
2.5.11. Convenio Iberoamericano de Cooperación sobre investigación, aseguramiento y obtención de prueba en materia de ciberdelincuencia, 2014 144
2.5.12. Décima Reunión de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas sobre Delito Cibernético, 2015 145

2.5.13. Décima Primera Reunión de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas sobre Delito Cibernético, 2021 145
2.6. Sistema de Naciones Unidas 146
2.6.1. VIII Congreso de las Naciones Unidas, sobre prevención del delito y tratamiento del delincuente, 1990 147
2.6.2. X Congreso de las Naciones Unidas, sobre prevención del delito y tratamiento del delincuente. La delincuencia y la justicia frente a los retos del siglo XXI, 2000 148
2.6.3. Resolución 55/63, sobre la lucha contra la utilización de la tecnología de la información con fines delictivos, 2000 150
2.6.4. Resolución 56/121, sobre la lucha contra la utilización de la tecnología de la información con fines delictivos, 2001 151
2.6.5. Resolución 64/211, sobre la creación de una cultura mundial de seguridad cibernética y balance de las medidas nacionales para proteger las infraestructuras de información esenciales, 2009 152
2.6.6. XII Congreso de las Naciones Unidas sobre Estrategias amplias ante problemas globales: Los sistemas de prevención del delito y justicia penal y su desarrollo en un mundo en evolución, 2010 153
2.6.7. XIII Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, 2015 154
2.6.8. Informe de la Reunión del Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético, 2020 156
2.6.9. XIV Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, 2021 158
2.6.10. La Convención de las Naciones Unidas contra la Ciberdelincuencia, 2024 159
2.7. Conclusiones del capítulo 164

CAPÍTULO 3
HISTORIA LEGISLATIVA DE LOS DELITOS CONTRA LA SEGURIDAD INFORMÁTICA

3.1. Introducción 169
3.2. Primer periodo: de 1991 al 2000 172
3.2.1. La interferencia telefónica (art. 162, CP), 1991 173
3.2.2. Tipificación de los delitos informáticos (arts. 207-A, 207-B y 207-C CP), 2000 174
3.3. Segundo periodo: del 2000 al 2013 179
3.3.1. Propuestas legislativas que no prosperaron 179
3.3.1.1. Periodo legislativo 2000-2001 179
3.3.1.2. Periodo legislativo 2001-2006 180
3.3.1.3. Periodo legislativo 2006-2011 185
3.3.2. Incorporación de nuevos delitos informáticos al Código Penal 188
3.3.2.1. Penalización de la clonación o adulteración de terminales de telefonía celular (art. 222-A, CP), 2006 188
3.3.2.2. Elusión de medidas tecnológicas, productos destinados a la elusión de medidas tecnológicas y servicios destinados a la elusión de medidas tecnológicas (arts. 220-A, 220-B y 220-C CP), 2008 190

3.4. Tercer periodo: del 2013 a diciembre del 2023 191
3.4.1. Tráfico ilegal de datos (art. 207-D, CP), 2013 191
3.4.2. Ley N.º 30096 o Ley de Delitos Informáticos, 2013 192
3.4.3. Modificación de la Ley N.º 30096 o Ley de Delitos Informáticos, 2014 .. 197
3.4.4. Periodo Legislativo 2016-2021 199
3.4.5. Adhesión del Perú al Convenio de Budapest, 2019 200
3.4.5.1. Declaraciones del Perú frente al Convenio de Budapest 200
3.4.5.2. Reservas del Perú frente al Convenio de Budapest 201
3.5. Cuarto periodo: de diciembre del 2023 a la actualidad 202
3.5.1. Modificaciones a la LDI: Decretos Legislativos 1591 y 1614, 2023 202
3.5.2. Incorporación de nuevos delitos a la LDI: Decreto Legislativo 1625 y Ley 32183, 2024 204
3.5.3. Suscripción del Segundo Protocolo Adicional al Convenio sobre la Ciberdelincuencia, 2024 205
3.5.4. Propuesta legislativa, 2024 206
3.6. Conclusiones del capítulo 207

CAPÍTULO 4
LA LEY DE DELITOS INFORMÁTICOS: CUESTIONES PRELIMINARES

4.1. Introducción 212
4.2. Funciones preventivas y retributivas de la LDI 213
4.3. Sistemas y datos informáticos 217
4.3.1. Sistemas informáticos 219
4.3.2. Datos informáticos 221
4.4. El uso de las TIC como medio comisivo 224
4.5. Bienes jurídicos protegidos en la LDI 228
4.6. La seguridad informática como bien jurídico protegido 231
4.6.1. Definición de *seguridad informática* 231
4.6.2. La seguridad informática como bien jurídico protegido 233
4.7. Elementos de la seguridad informática y actividad delictiva 242
4.7.1. Confidencialidad 245
4.7.2. Integridad 245
4.7.3. Disponibilidad 246
4.8. Actuación deliberada e ilegítima 249
4.8.1. Actuación deliberada 250
4.8.2. Actuación ilegítima 256
4.9. Ser *hacker* no significa ser ciberdelincuente 260
4.9.1. El tratamiento del término *hacker* en los medios de comunicación 263
4.9.2. Breves reflexiones sobre sesgos y prejuicios 273
4.9.3. Los sesgos y prejuicios pueden afectar la investigación criminal y la toma de decisiones 275
4.10. Conclusiones del capítulo 278

CAPÍTULO 5
ACCESO ILÍCITO O INTRUSISMO INFORMÁTICO

5.1. Introducción 284
5.2. Regulación en el Convenio sobre la Ciberdelincuencia 289
5.3. Regulación en la Convención de las Naciones Unidas contra la Ciberdelincuencia . 292
5.4. Legislación comparada 293
5.5. Legislación nacional 297
5.5.1. Antecedentes normativos 297
5.5.2. Génesis legislativa 299
5.5.3. Evolución legislativa 299
5.5.4. Regulación actual 301
5.6. El bien jurídico penalmente protegido 305
5.7. El tipo penal de acceso ilícito 311
5.7.1. Elementos comunes 316
5.7.1.1. Sujetos 316
5.7.1.2. Tipo subjetivo 319
5.7.2. Las modalidades de acceso ilícito 323
5.7.2.1. Sin vulneración de medidas de seguridad 323
5.7.2.1.1. Acceso 324
5.7.2.1.2. Exceso 325
5.7.2.2. Con vulneración de medidas de seguridad 329
5.7.2.2.1. Acceso con vulneración de medidas de seguridad .. 338
5.8. Las situaciones de justificación en el delito de acceso ilícito 345
5.8.1. *Penetration test* y *vulnerability assessment* 346
5.8.2. ¿Acceso ilícito en ejercicio de la patria potestad? 349
5.9. Consumación 351
5.10. Concursos 353
5.11. Penalidad 356
5.12. Circunstancias agravantes 357
5.13. Propuesta normativa 361
5.14. Conclusiones del capítulo 362

CAPÍTULO 6
ATENTADO A LA INTEGRIDAD DE DATOS INFORMÁTICOS

6.1. Introducción 367
6.2. Regulación en el Convenio sobre la Ciberdelincuencia 370
6.3. Regulación en la Convención de las Naciones Unidas contra la Ciberdelincuencia . 372
6.4. Legislación comparada 373
6.5. Legislación nacional 376
6.5.1. Antecedentes normativos 377
6.5.2. Génesis legislativa 378
6.5.3. Evolución legislativa 379

6.5.4. Regulación actual 380
6.6. El bien jurídico penalmente protegido 382
6.7. Tipicidad objetiva 384
6.7.1. Sujetos 384
6.7.2. Acciones típicas 386
6.7.2.1. Dañar, *damaging* 389
6.7.2.2. Introducir 390
6.7.2.3. Borrar, *deletion* 391
6.7.2.4. Deteriorar, *deterioration* 395
6.7.2.5. Alterar, *altering* 396
6.7.2.6. Suprimir, *suppressing* 399
6.7.2.7. Hacer inaccesible 402
6.7.3. Objeto del delito: datos informáticos 405
6.8. Tipicidad subjetiva 406
6.9. Las situaciones de justificación en el delito de atentado contra los datos informáticos 407
6.10. Consumación 416
6.11. Concursos 418
6.12. Penalidad 421
6.13. Circunstancias agravantes 422
6.14. Propuesta normativa 424
6.15. Conclusiones del capítulo 425

CAPÍTULO 7
ATENTADO A LA INTEGRIDAD DE SISTEMAS INFORMÁTICOS

7.1. Introducción 432
7.2. Regulación en el Convenio sobre la Ciberdelincuencia 440
7.3. Regulación en la Convención de las Naciones Unidas contra la Ciberdelincuencia . 442
7.4. Legislación comparada 443
7.5. Legislación nacional 446
7.5.1. Antecedentes normativos 446
7.5.2. Génesis legislativa 447
7.5.3. Evolución legislativa 449
7.5.4. Regulación actual 449
7.6. El bien jurídico penalmente protegido 451
7.7. Tipicidad objetiva 456
7.7.1. Sujetos 456
7.7.2. Acción típica 458
7.7.2.1. Inutilizar 459
7.7.2.2. Impedir (el acceso) 463
7.7.2.3. Entorpecer 465
7.7.2.4. Imposibilitar 467
7.7.3. Objeto del delito 468
7.7.3.1. Funcionamiento 469
7.7.3.2. Prestación de servicios 470

7.8. Tipicidad subjetiva 470
7.9. Las situaciones de justificación en el delito de atentado a la integridad de sistemas informáticos 471
7.10. Consumación 473
7.11. Concursos 474
7.12. Penalidad 479
7.13. Circunstancias agravantes 479
7.14. Propuesta normativa 484
7.15. Conclusiones del capítulo 485

CAPÍTULO 8
INTERCEPTACIÓN ILÍCITA DE DATOS INFORMÁTICOS

8.1. Introducción 490
8.2. Regulación en el Convenio sobre la Ciberdelincuencia 492
8.3. Regulación en la Convención de las Naciones Unidas contra la Ciberdelincuencia . 496
8.4. Legislación comparada 496
8.5. Legislación nacional 499
8.5.1. Antecedentes normativos 499
8.5.2. Génesis legislativa 501
8.5.3. Evolución legislativa 503
8.5.4. Regulación actual 504
8.6. El bien jurídico penalmente protegido 510
8.7. Tipicidad objetiva 513
8.7.1. Sujetos 513
8.7.2. Acciones típicas 514
8.7.2.1. Interceptar 514
8.7.3. Objeto del delito: datos informáticos y emisiones electromagnéticas 517
8.7.3.1. En transmisiones no públicas 517
8.7.3.2. Origen de las transmisiones 518
8.7.3.3. Emisiones electromagnéticas 521
8.7.4. Circunstancias agravantes específicas 523
8.7.4.1. Por el tipo de información 523
8.7.4.2. Por el riesgo que representa 525
8.7.4.3. Por la condición del agente 526
8.8. Tipicidad subjetiva 527
8.9. Las situaciones de justificación en el delito de interceptación ilícita de datos informáticos 527
8.9.1. Registro remoto de equipos informáticos 528
8.10. Consumación 531
8.11. Concursos 532
8.12. Penalidad 533
8.13. Circunstancias agravantes 534
8.14. Propuesta normativa 535
8.15. Conclusiones del capítulo 536

CAPÍTULO 9
ABUSO DE MECANISMOS Y DISPOSITIVOS INFORMÁTICOS

9.1. Introducción 542
9.2. Regulación en el Convenio sobre la Ciberdelincuencia 545
9.3. Regulación en la Convención de las Naciones Unidas contra la Ciberdelincuencia . 550
9.4. Legislación comparada 551
9.5. Legislación nacional 554
9.5.1. Antecedentes normativos 554
9.5.2. Génesis legislativa 554
9.5.3. Evolución legislativa 556
9.5.4. Regulación actual 558
9.6. El bien jurídico penalmente protegido 560
9.7. Tipicidad objetiva 563
9.7.1. Sujetos 563
9.7.2. Acción típica 563
9.7.2.1. Fabricar 564
9.7.2.2. Diseñar 566
9.7.2.3. Desarrollar 567
9.7.2.4. Vender 569
9.7.2.5. Facilitar 571
9.7.2.6. Distribuir 573
9.7.2.7. Importar 574
9.7.2.8. Obtener 576
9.7.3. Objeto del delito: ¿mecanismos y dispositivos informáticos? 577
9.7.3.1. Mecanismos 578
9.7.3.2. Programas informáticos 579
9.7.3.3. Dispositivos 579
9.7.3.4. Contraseñas 580
9.7.3.5. Códigos de acceso 580
9.7.3.6. Cualquier otro dato informático 581
9.7.3.7. La finalidad maliciosa como única función 583
9.8. Tipicidad subjetiva 584
9.9. Las situaciones de justificación en el delito de abuso de mecanismos y dispositivos informáticos 586
9.10. Consumación 587
9.11. Concursos 590
9.12. Penalidad 590
9.13. Circunstancias agravantes 591
9.14. Propuesta normativa 592
9.15. Conclusiones del capítulo 593

CAPÍTULO 10
ESTUDIO DE PROYECTOS DE LEY RELACIONADOS A LOS CIBERDELITOS CONTRA LA SEGURIDAD INFORMÁTICA

10.1. Introducción 600
10.2. Proyecto de Ley N.º 5071/99-CR, Ley de Delitos Informáticos 602
10.2.1. Fórmula legal 602
10.2.2. Exposición de motivos 602
10.2.3. Comentarios 602
10.3. Proyecto de Ley N.º 5132/99-CR, Ley que propone establecer como figura típica penal los delitos informáticos 604
10.3.1. Fórmula legal 604
10.3.2. Considerando / exposición de motivos 605
10.3.3. Comentarios 605
10.4. Proyecto de Ley N.º 1744/2000, Ley que modifica los arts. 207-A, 207-B y 207-C del Título V del Libro II del Código Penal, DL 635 referente a los delitos informáticos 608
10.4.1. Fórmula legal 608
10.4.2. Considerando / exposición de motivos 609
10.4.3. Comentarios 609
10.5. Proyecto de Ley N.º 2226/2002-CR, Ley que modifica los arts. 207-A, 207-B y 207-C del Título V del Libro II del Código Penal, DL 635 referente a los delitos informáticos 611
10.5.1. Fórmula legal 611
10.5.2. Considerando / exposición de motivos 612
10.5.3. Comentarios 612
10.6. Proyecto de Ley N.º 7197/2003-CR, Ley que incorpora nuevas figuras delictivas al Código Penal sobre los delitos informáticos 614
10.6.1. Fórmula legal 614
10.6.2. Exposición de motivos 615
10.6.3. Comentarios 615
10.7. Proyecto de Ley N.º 10079/2003-CR, Ley que modifica el art. 207-B y agrega al Capítulo X (Delitos Informáticos) del Título V del Código Penal, los arts. 207-D, 207-E, 207-F y 207-G 616
10.7.1. Fórmula legal 616
10.7.2. Exposición de motivos 618
10.7.3. Comentarios 618
10.8. Proyecto de Ley N.º 11346/2004-CR, Ley que incorpora nuevas figuras delictivas al Código de Justicia Militar 620
10.8.1. Fórmula legal 621
10.8.2. Exposición de motivos 621
10.8.3. Comentarios 622
10.9. Proyecto de Ley N.º 11402/2004-CR, Ley que modifica el art. 207-A del Código Penal referido a los delitos informáticos 623
10.9.1. Fórmula legal 623
10.9.2. Exposición de motivos 624

10.9.3. Comentarios 624
10.10. Proyecto de Ley N.º 1318/2006-CR, Ley de represión de los delitos informáticos .. 625
10.10.1. Fórmula legal 625
10.10.2. Exposición de motivos 627
10.10.3. Comentarios 627
10.11. Proyecto de Ley N.º 1828/2007-CR, Ley que penaliza los delitos informáticos . 630
10.11.1. Fórmula legal 630
10.11.2. Exposición de motivos 637
10.11.3. Comentarios 637
10.12. Proyecto de Ley N.º 3083/2008-CR, Ley que regula los delitos informáticos 639
10.12.1. Fórmula legal 639
10.12.2. Comentarios 639
10.13. Proyecto de Ley N.º 4279/2010-CR, Ley que propone crear un sistema regulador y sancionador respecto al uso de Tecnologías de Información y Comunicación (TICs) 640
10.13.1. Fórmula legal 640
10.13.2. Exposición de motivos 641
10.13.3. Comentarios 641
10.14. Proyecto de Ley N.º 34/2011-CR, Ley que regula los Delitos Informáticos 642
10.14.1. Fórmula legal 642
10.14.2. Exposición de motivos 646
10.14.3. Comentarios 646
10.15. Proyecto de Ley N.º 307/2011-CR, Ley especial sobre Delitos cometidos con el uso de las Tecnologías de la Información y Comunicación 651
10.15.1. Fórmula legal 651
10.15.2. Exposición de motivos 652
10.15.3. Comentarios 652
10.16. Proyecto de Ley N.º 1136/2011-CR, Ley que modifica el art. 207-C del Código Penal, incorporando el delito de robo de identidad virtual e incorpora el art. 207-D, delito informático agravado 654
10.16.1. Fórmula legal 654
10.16.2. Exposición de motivos 655
10.16.3. Comentarios 655
10.17. Proyecto de Ley N.º 1257/2011-CR, Ley que agrava los delitos de violación del secreto de las comunicaciones 655
10.17.1. Fórmula legal 655
10.17.2. Exposición de motivos 656
10.17.3. Comentarios 657
10.18. Proyecto de Ley N.º 2129/2012-CR, Ley que sanciona la venta ilegal de bases de datos y datos personales de usuarios y consumidores 657
10.18.1. Fórmula legal 657
10.18.2. Exposición de motivos 658
10.18.3. Comentarios 658
10.19. Proyecto de Ley N.º 2520/2012-PE, Ley de Represión de la Cibercriminalidad .. 659
10.19.1. Fórmula legal 659
10.19.2. Exposición de motivos 662
10.19.3. Comentarios 662

10.20. Proyecto de Ley N.º 2991/2013-CR, Ley que modifica la Ley N.º 30096, Ley de Delitos Informáticos 665
10.20.1. Fórmula legal 665
10.20.2. Exposición de motivos 667
10.20.3. Comentarios 667
10.21. Proyecto de Ley N.º 2999/2013-CR, Ley que modifica, incorpora y deroga diversos artículos a la Ley N.º 30096, Ley de Delitos Informáticos 669
10.21.1. Fórmula legal 669
10.21.2. Exposición de motivos 671
10.21.3. Comentarios 671
10.22. Proyecto de Ley N.º 3105/2013-CR, Ley que modifica la Ley N.º 30096, Ley de Delitos Informáticos 671
10.22.1. Fórmula legal 671
10.22.2. Exposición de motivos 673
10.22.3. Comentarios 673
10.23 Proyecto de Ley N.º 3980/2014-CR, Ley que propone modificar la Ley N.º 30096, Ley de Delitos Informáticos, modificada por la Ley N.º 30171 673
10.23.1 Fórmula legal 674
10.23.2 Exposición de motivos 674
10.23.3 Comentarios 674
10.24. Proyecto de Ley N.º 5630/2020-CR, Ley de seguridad informática y represión de los delitos informáticos 675
10.24.1. Fórmula legal 675
10.24.2. Exposición de motivos 677
10.24.3. Comentarios 677
10.25. Proyecto de Ley N.º 9136/2024-CR, Ley que modifica la Ley de Delitos Informáticos respecto a la activación y posesión ilegal de SIM *Cards* 678
10.25.1. Fórmula legal 678
10.25.2. Exposición de motivos 679
10.25.3. Comentarios 679
10.26. Proyecto de Ley N.º 9443/2024-CR, Ley que protege a los peruanos frente a las amenazas cibernéticas 680
10.26.1. Fórmula legal 680
10.26.2. Exposición de motivos 681
10.26.3. Comentarios 682

Epílogo 683

ANEXOS

Anexo A. Línea de tiempo de los ciberdelitos contra la seguridad informática 689
Anexo B. Dictamen de la Comisión Ad Hoc de Justicia y Derechos Humanos, recaído en los proyectos de ley N.ºs 034/2011-CR, 307/2011-CR y 1136/2011-CR 692
Anexo C. Diario de debates, 12 de setiembre del 2013 692
Anexo D. La enseñanza de la ciberdelincuencia en la educación superior 692

BIBLIOGRAFÍA 721

II. ÍNDICE DE CASOS

Caso 1.	Lockbit 3.0 compromete datos policiales y exige rescate	26
Caso 2.	Primera muerte producto de un ataque de *ransomware*	27
Caso 3.	Gerente de centro geriátrico accede al ordenador de enfermera	68
Caso 4.	Pedro espió el WhatsApp de Lorenza y fue condenado por violencia de género	68
Caso 5.	Sixto creó una bomba lógica y perjudicó más de tres computadoras de una entidad financiera	69
Caso 6.	*Insider* de una cooperativa financiera expuso más de 2,7 millones de registros	70
Caso 7.	Los ataques DDoS alcanzan niveles récord, con 398 millones de RPS	71
Caso 8.	Luis Pablo usó *phishing* para robar datos bancarios, obtuvo más de 600 mil euros, pero fue condenado	71
Caso 9.	Detectan dominios falsos con NFT usados para *phishing* y *malware*	72
Caso 10.	Profesor de música es condenado por *grooming*	72
Caso 11.	Atacantes afines a Ucrania y Rusia libran una guerra en el ciberespacio	73
Caso 12.	Nullbuge81 hackea los sistemas informáticos de Disney	74
Caso 13.	Vásquez y Vergara fueron condenados por apropiarse de 9600 soles de una cuenta del BCP mediante *pharming*	75
Caso 14.	Julio César y Cecilio fueron víctimas de SMShing	76
Caso 15.	Troyano Poco Rat se distribuye entre empresas de los sectores de minería, manufactura, hotelería y servicios públicos en países de habla hispana	77
Caso 16.	Nuria fue víctima de *phishing*; Joaquina condenada como *mula* bancaria	77
Caso 17.	Operativo policial Galácticos desarticula organización que estafaba mediante ataques de ingeniería social en España	78
Caso 18.	Estafa, a través de subastas de productos no entregados, en plataforma de comercio electrónico eBay	79
Caso 19.	Acusado de crear el virus Kelar es absuelto	80
Caso 20.	Uso de *sniffer* para descubrir quien accede a información confidencial	80
Caso 21.	Grupo de ciberdelincuentes dirigen ataques de ciberespionaje corporativo contra entidades ubicadas en Australia, Canadá, Alemania, Rusia, Eslovenia, Reino Unido, Ucrania y Estados Unidos	81
Caso 22.	Se imponen sanciones contra responsables de WannaCry, NotPetya y Operation Cloud Hopper	81
Caso 23.	Crean cuenta falsa de congresista fujimorista Tania Ramírez García en red social X	82
Caso 24.	Sentencian a 3 años y 20 días de pena suspendida a mujer que suplantó la identidad de otra en Facebook	83
Caso 25.	Campaña de distribución de *malware*, a través de correos electrónicos supuestamente enviados por DHL	84
Caso 26.	¿Cómo opera el DNS *spoofing*?	85
Caso 27.	¿Cómo opera el ARP *spoofing*?	86
Caso 28.	Rosendo es absuelto al no descartarse que fue víctima de IP *spoofing*	86
Caso 29.	Germán es víctima de *web spoofing* y Concepción es condenado	87
Caso 30.	Cárteles mexicanos utilizan criptomonedas para minimizar el riesgo de ser descubiertos	88
Caso 31.	Grupo Qilin afecta centros de salud con ataques de *ransomware*	89

Caso 32. Samuel es condenado por actos de ciberextorsión contra diferentes agraviadas. 90
Caso 33. Usuarios del Banco de Crédito del Perú son víctimas de *cybersquatting*... 91
Caso 34. Hyalmar Laynes es investigado por ciberacoso en agravio de diversas periodistas peruanas. 91
Caso 35. Demandan a padres de agresor por actos de *cyberbullying* en la escuela. 92
Caso 36. Agresor es condenado por enviar decenas de mensajes y audios por WhatsApp a su víctima. 93
Caso 37. Daniel es condenado por enviar fotografías íntimas de su expareja, vía Instagram y Facebook 94
Caso 38. Víctima de sextorsión se suicida en Nueva Gales; sus agresores vivían en Nigeria. 95
Caso 39. Pese a cuestionamientos sobre la prueba, Mauricio fue condenado por *grooming* 95
Caso 40. El grupo de ciberdelincuentes Guacamaya Roja afirma haber hackeado los sistemas informáticos policiales y militares de México, Perú, Salvador, Chile y Colombia 96
Caso 41. Hipólito fue condenado por el delito de distribución de imágenes de explotación sexual infantil en una investigación que se inició a partir del aviso de la Homeland Security Investigations. 97
Caso 42. Administrador de webs retransmitió partidos sin autorización; fue condenado por delito contra la propiedad intelectual. 98
Caso 43. Aureliano, Camila, Angustia, Carlota, Apolonia, Alberto, Ascensión, Bartolomé, Benigno y Cándido fueron condenados por mensajes de odio publicados en Facebook. 99
Caso 44. Braulio fue condenado por adoctrinamiento terrorista, a través de redes sociales. 100
Caso 45. Imanol e Isaac fueron condenados por enaltecimiento terrorista a través TikTok, Facebook e Instagram. 101
Caso 46. El primer ataque informático de la historia fue cometido por un mago que interceptó mensajes inalámbricos en una demostración pública. 108
Caso 47. El primer *hacker* de la historia, René Carmille saboteó censo nazi, protegiendo judíos. 108
Caso 48. El primer virus informático Creeper o Enredadora surgió en 1971. 109
Caso 49. El impacto del gusano ILoveYou. 169
Caso 50. Víctima de hackeo denuncia el suceso en la Policía, pero fiscalía archiva investigación liminarmente. 285
Caso 51. Actriz Carolina Dieckmann fue víctima de acceso ilícito: su caso motivó la tipificación de los delitos informáticos en Brasil. 288
Caso 52. Periodista se infiltra en grupo de Telegram y descubre que ciberdelincuentes podían alterar bases de datos de la Policía peruana. 303
Caso 53. La web del Instituto Nacional de Defensa Civil fue utilizada para distribuir troyanos entre sus visitantes 304
Caso 54. Trabajador accede, sin autorización, a *smart TV* instalada en el directorio de un estudio jurídico. 312
Caso 55. ¿Acceder a un PlayStation protegido por una contraseña configura el delito de acceso ilícito? 313
Caso 56. Estudiante universitario accede al registro de notas, sin autorización, para conocer cuánto obtuvo en el examen. 313

Caso 57. Sin autorización, accede al teléfono de su pareja para ver las fotografías tomadas durante un día de excursión. 313
Caso 58. Nam3L3ss publicó más de 2,8 millones de líneas de datos de empleados de Amazon. 318
Caso 59. Pedro usa la clave de Antonio para acceder a los sistemas de la empresa, sin saber que fue despedido. 322
Caso 60. Enfermera de atención primaria accede y visualiza las historias clínicas de sus compañeros. 326
Caso 61. Telegram activó un programa de recompensas por errores de su plataforma. 328
Caso 62. Gary McKinnon accedió ilegalmente a sistemas de la NASA buscando evidencia extraterrestre; Reino Unido rechazó su extradición. 335
Caso 63. El sistema de detección de intrusos de la empresa advierte la presencia de un ciberdelincuente e impide su acceso. 352
Caso 64. Ciberdelincuente emplea ataque de fuerza bruta para acceder a sistema informático. 352
Caso 65. Jorge ingresa, a través de Google, a su banco de confianza, pero es víctima de fraude informático. 354
Caso 66. Narcotraficantes contratan ciberdelincuentes para infiltrarse en sistemas informáticos y localizar sus cargamentos. 358
Caso 67. Ciberdelincuentes contratan *insiders* para obtener acceso a las redes de telecomunicaciones y datos de abonados. 358
Caso 68. Las actuaciones del grupo Turla ponen en riesgo la confidencialidad de entidades diplomáticas de diferentes países. 359
Caso 69. Donald Gene Burleson fue condenado por utilizar un *malware* para eliminar 168 mil registros, luego de ser despedido. 368
Caso 70. Ciberdelincuentes utilizan el *ransomware* NotPetya y originan uno de los ciberataques más costosos de la historia. 368
Caso 71. Explotan vulnerabilidad en WD My Book y borran archivos con ataques zero-day. 393
Caso 72. El *malware* Shamoon atacó petrolera saudí en 2012, borrando datos y afectando suministro global. 394
Caso 73. Ataque de *defacement* alteró la web municipal de Ate, Lima. 398
Caso 74. Deface Perú ataca la página web de la Municipalidad de Pucusana. 399
Caso 75. Troyanos ocultan archivos de USB infectado. 400
Caso 76. Martín envía los archivos de trabajo de su compañero Leopoldo a la papelera de reciclaje. 401
Caso 77. *Ransomware* Vovalex se propagó disfrazado de aplicaciones de optimización. 403
Caso 78. Severino y Carlos Jesús modificaron sus calificaciones en los sistemas informáticos de su centro de estudios. 405
Caso 79. La Universidad de Tolima reportó que un ciberdelincuente modificó las notas de todos sus alumnos. 406
Caso 80. En Argentina, Joaquín Sorianello expuso falla electoral electrónica y fue procesado. Finalmente, consiguió su absolución. 408
Caso 81. Anonymous se enfrenta a Los Zetas por el secuestro de uno de sus integrantes. 412
Caso 82. Modifican datos del sistema informático del Ministerio de Transporte y Comunicaciones para que un conductor obtenga su licencia de conducir. 419

Caso 83. La organización Wizard Spider distribuye el *ransomware* Ryuk y pide millonarios rescates. 422
Caso 84. Ciberdelincuentes ofrecen cambiar notas en centros educativos, a cambio de dinero. 423
Caso 85. Las periodistas Juliana Oxenford y Rosa María Palacios pierden acceso a sus cuentas en X, en las que tenían millones de seguidores..... 432
Caso 86. Ciberdelincuentes utilizaron el *malware* SYS01 para robar credenciales, *cookies* y datos de cuentas comerciales. 434
Caso 87. Ciberdelincuentes atacan la cuenta de la Biblioteca Nacional del Perú en la red social X. 435
Caso 88. La organización The Dark Storm Team dirigió un ataque de denegación de servicio contra la red social X. 437
Caso 89. Ciberataques dirigen ataque de *ransomware* contra el Colegio de Abogados de Lima. 438
Caso 90. Vishwanath Akuthota fue condenado por utilizar un *USB killer* para dañar 66 computadoras de un centro educativo de Nueva York..... 455
Caso 91. Juan fue condenado por emplear un *USB killer* y dañar dispositivos informáticos del Instituto de Biología y Genética Molecular de España..... 455
Caso 92. Script Kiddie Matrix ofrece ataques de denegación de servicios en grupos de Telegram..... 457
Caso 93. *Wipers* de diferentes cepas son utilizados contra Ucrania. 460
Caso 94. *Malware* Stuxnet es utilizado para atacar y destruir máquinas centrifugadoras de centrales nucleares. 461
Caso 95. Banco Santander Chile sufrió un ataque de denegación de servicios, lo que originó que sus usuarios no pudiesen acceder a las plataformas financieras. 464
Caso 96. Se descubren ataques de *ransomware* que podrían afectar *smart TVs*. 465
Caso 97. *Malware* Pro-Ocean se propagó mediante vulnerabilidades en la nube, utilizando dispositivos infectados para minar criptomonedas..... 466
Caso 98. *Ransomware* afectó a Blue Yonder, paralizando servicios para Starbucks y otras empresas..... 468
Caso 99. Sustituye tarjetas de memoria para que no proyecte su exposición. 469
Caso 100. Ciberataque con *malware* Black Energy origina apagones masivos en Ucrania. 470
Caso 101. Ejecutivo de banca personal del BBVA Banco Continental utilizó documentos falsos para manipular los sistemas informáticos y obtener 12 tarjetas de crédito..... 477
Caso 102. Trabajador de una entidad financiera empleó un *skimmer* para clonar las tarjetas de créditos de sus clientes..... 478
Caso 103. En la operación internacional QuickSand se desarticuló a la organización REvil Sodinokibi. 480
Caso 104. Un grupo de personas distribuían mensajes falsos de la Policía española para que las víctimas ingresen a un enlace y descarguen un *malware*. 482
Caso 105. Grupo CloAk Ransomware atacó al Foro Militar Policial, ofreciendo a la venta 221 GB de datos..... 482
Caso 106. ¿Cómo funciona el *malware* AirHopper?..... 490
Caso 107. Preocupación mundial por la distribución del *spyware* Pegasus. 490
Caso 108. Ataque de intermediario como manifestación del delito de interceptación ilícita de datos informáticos..... 515

Caso 109. Troyano LodaRAT se propagó vía *phishing*, espiando usuarios y robando credenciales en Android y Windows. 516
Caso 110. Policía Federal Australiana arrestó a un hombre que instaló redes wifi falsas para interceptar credenciales. 520
Caso 111. *Van Eck* es un tipo de ataque de espionaje que analiza la radiación electromagnética. 521
Caso 112. FBI alertó sobre cargadores USB que escondían *keyloggers*. 521
Caso 113. Gusano infectó 55,000 ordenadores, robando datos de entidades gubernamentales y militares en 39 países. 525
Caso 114. Organización APT33 realizó ataques de ciberespionaje contra empresas del sector de la aviación, militar, comercial y energético. 526
Caso 115. La evolución del *malware* bancario EMOTET. 532
Caso 116. Operación Talent desmanteló Cracked y Nulled, dos mercados ilegales que registraban más de 10 millones de usuarios. 543
Caso 117. Julián construye *USB killer* a partir de planos que encontró en un foro de ciberseguridad. 565
Caso 118. CrimeEnforcers, una compañía que diseña soluciones (ilegales) para sus *clientes* que operan en el mercado negro. 566
Caso 119. SpyEye, el *malware* que elimina a la competencia alojada en el dispositivo infectado. 568
Caso 120. La evolución de negocios como CallService.biz: de ofrecer *callcenters* ilegales a fabricar *malware*. 569
Caso 121. Zeus Builder, Bugat y SpyEye a la venta en el mercado ilegal. 570
Caso 122. Deface Perú publica credenciales de acceso a una corte de justicia peruana. 572
Caso 123. Cuatro jóvenes peruanos importan cables OMG que permiten interceptar datos informáticos. 575
Caso 124. Juan Diego compró *software* malicioso con autorización de su jefe, pero enfrenta problemas probatorios. 587

III. ÍNDICE DE CUADROS

Cuadro 1: Generaciones que integran el tránsito de las TIC. 49
Cuadro 2: Actividades que realiza la población usuaria de internet, al primer trimestre de 2024. 51
Cuadro 3: Puntos de inflexión que ocurrirá antes de 2025. 52
Cuadro 4: Años de nacimiento de las generaciones. Elaboración propia. 55
Cuadro 5. Modalidades de cibercrimen. Elaborado por Fernando Miró Llinares. 67
Cuadro 6. Legislación comparada inicial (1973 a 1989). Elaboración propia. 116
Cuadro 7: Cuadro resumen del Convenio de Budapest y del informe explicativo. Elaboración propia. 127
Cuadro 8: Estados adherentes e invitados a suscribir el Convenio de Budapest, al 31 de diciembre de 2024. 128
Cuadro 9: Estados latinoamericanos que se adhirieron al Convenio de Budapest, al 2024. 129

Cuadro 10: Cuadro resumen de la Convención de las Naciones Unidas contra la ciberdelincuencia. Elaboración propia. 164
Cuadro 11. Cuadro resumen de los ciberdelitos contra la seguridad informática recogidos en la LDI. Elaboración propia. 199
Cuadro 12. Cuadro resumen de los delitos que recogen el elemento *deliberadamente* en el Código Penal. 251
Cuadro 13. Cuadro resumen de los delitos que recogen el elemento deliberadamente en la LDI. 254
Cuadro 14. Cuadro resumen de los delitos recogen el elemento *ilegítimamente* en la LDI. 257
Cuadro 15. Legislación comparada respecto al delito de acceso ilícito. Elaboración propia. 295
Cuadro 16. Regulación del delito de acceso ilícito, 2013-2024. Elaboración propia. 305
Cuadro 17. Las 20 contraseñas más usuales, empleadas a nivel mundial en el 2024. 334
Cuadro 18. Informe técnico. Elaborado por Luis Angulo Aguirre. 348
Cuadro 19. Legislación comparada respecto al delito de atentado a la integridad de datos informáticos. Elaboración propia. 375
Cuadro 20. Regulación del delito de atentado contra la integridad de datos informáticos, 2013-2024. Elaboración propia. 380
Cuadro 21. Comparación de los verbos rectores recogidos en el artículo 4 del Convenio de Budapest, el artículo 9 de la Convención de las Naciones Unidas contra la Ciberdelincuencia y en el artículo 3 de la LDI. Elaboración propia. 381
Cuadro 22. Resumen de definiciones propuestas de los verbos que integran delito de atentado a la integridad de datos informáticos. Elaboración propia. 404
Cuadro 23. Legislación comparada respecto al delito de atentado a la integridad de sistemas informáticos. Elaboración propia. 444
Cuadro 24. Regulación del delito de atentados contra la integridad de sistemas informáticos, 2013-2024. Elaboración propia. 450
Cuadro 25. Comparación de los verbos rectores recogidos en el artículo 5 del Convenio de Budapest, en el artículo 10 de la Convención de las Naciones Unidas contra la Ciberdelincuencia y en el artículo 4 de la LDI. Elaboración propia. 450
Cuadro 26. Resumen de definiciones propuestas de los verbos que integran delito de atentado a la integridad de sistemas informáticos. Elaboración propia. 468
Cuadro 27. Legislación comparada respecto al delito de interceptación ilícita de datos informáticos. Elaboración propia. 498
Cuadro 28. Comparación de la sanción prevista en los delitos de interferencia telefónica, interferencia de comunicaciones electrónicas e interceptación de datos informáticos. Elaboración propia. 508
Cuadro 29. Regulación del delito de interceptación ilegal de datos informáticos, 2013-2024. Elaboración propia. 509
Cuadro 30. Diferencia de verbos rectores de los delitos previstos en los artículos 162, 162-B CP y 7 LDI. 515
Cuadro 31. Información secreta, según el TUO de la Ley 27806. Elaboración propia. 523
Cuadro 32. Información reservada, según el TUO de la Ley N.º 27806. Elaboración propia. 524
Cuadro 33. Información confidencial, según el TUO de la Ley N.º 27806. Elaboración propia. 525

Cuadro 34. Legislación comparada respecto al abuso de mecanismos y dispositivos informáticos. Elaboración propia. 553
Cuadro 35. Regulación del delito de abuso de mecanismos y dispositivos informáticos, 2013-2024. Elaboración propia. 558
Cuadro 36. Comparación de los verbos rectores recogidos en el artículo 6 del Convenio de Budapest, el artículo 11 de la Convención de las Naciones Unidas sobre la Ciberdelincuencia y el artículo 10 de la LDI. Elaboración propia. 559
Cuadro 37. Sistematización de los ciberdelitos contra la seguridad informático, según el bien jurídico afectado específicamente. Elaboración propia. 562
Cuadro 38. Resumen de las definiciones propuestas de los verbos que integran el delito de abuso de mecanismos y dispositivos informáticos. Elaboración propia. 577
Cuadro 39. Resumen de las definiciones propuestas de los objetos delictivos que integran el delito de abuso de mecanismos y dispositivos informáticos. Elaboración propia. 582

IV. ÍNDICE DE DIAGRAMAS

Diagrama 1. Esquema de ataque por envenenamiento de DNS. Elaboración propia. 85
Diagrama 2. Esquema de ataque por ARP *spoofing*. Elaboración propia. 86
Diagrama 3. Tipos de delitos informáticos (*computer abuse*). Elaborado por Donn B. Parker. 111
Diagrama 4. Trinomio CIA, por sus siglas en inglés. Elementos de la seguridad informática. 244
Diagrama 5. Relación de los delitos informáticos con los principales elementos de la seguridad informática que afectan. Elaboración propia. 248
Diagrama 6. Estructura del delito de acceso ilícito, propuesto en el Convenio de Budapest. Elaboración propia. 290
Diagrama 7. Estructura actual del delito de acceso ilícito, en el sistema penal peruano. Elaboración propia. 312
Diagrama 8. Elementos de seguridad que puede adoptar un usuario. Adaptación. 330
Diagrama 9. Ataque de exfiltración de datos. Adaptación. 360
Diagrama 10. Estructura del delito de ataque a la integridad de los datos, propuesto en el Convenio de Budapest. Elaboración propia. 370
Diagrama 11. Estructura actual del delito de atentado contra la integridad de datos informáticos, en el sistema penal peruano. Elaboración propia. 381
Diagrama 12. Solicitud de ejemplo, vista desde el servidor controlado por el atacante desde la víctima My Book Live. Adaptación, a partir de CENSYS. 394
Diagrama 13. Estructura del *malware* SYS01. Adaptación . 435
Diagrama 14. Estructura del delito de ataque a la integridad del sistema, propuesto en el Convenio de Budapest. Elaboración propia. 440
Diagrama 15. Estructura actual del delito de atentado contra la integridad de sistemas informáticos, en el sistema penal peruano. Elaboración propia. 451
Diagrama 16. Funcionamiento del *malware* Pro-Ocean. 467

Diagrama 17. Estructura del delito de interceptación ilícita, propuesto en el Convenio de Budapest. Elaboración propia 493
Diagrama 18. Relación de los delitos de interferencia telefónica (art. 162 CP), interferencia de comunicaciones electrónicas (art. 162-B CP) e interceptación ilegal de datos informáticos (art. 7 LDI). Elaboración propia. 508
Diagrama 19. Estructura actual del delito de interceptación ilegal de datos informáticos en el sistema penal peruano. Elaboración propia 510
Diagrama 20. ¿Cómo funciona un ataque de intermediario? 516
Diagrama 21. Estructura del delito de abuso de los dispositivos, propuesto en el Convenio de Budapest. Elaboración propia 546
Diagrama 22. Estructura actual del delito de abuso de dispositivos y mecanismos informáticos, en el sistema penal peruano. Elaboración propia. 560
Diagrama 23. Estructura del delito de acceso ilícito, propuesto en el PL N.º 5071/99-CR. Elaboración propia. 603
Diagrama 24. Estructura de los delitos de daños y sabotaje informático, propuestos en el PL N.º 5071/99-CR. Elaboración propia. 604
Diagrama 25. Estructura del delito de sabotaje informático, propuesto en el PL N.º 5132/99-CR. Elaboración propia. 606
Diagrama 26. Estructura de los delitos de acceso e interceptación ilícita, propuestos en el PL N.º 5132/99-CR. Elaboración propia 606
Diagrama 27. Estructura del delito de daños informáticos, propuesto en el PL N.º 5132/99-CR. Elaboración propia. 607
Diagrama 28. Estructura del delito de revelación de datos informáticos, propuesto en el PL N.º 5132/99-CR. Elaboración propia. 607
Diagrama 29. Estructura del delito de acceso ilícito y sabotaje informático (alteración), propuesto en el PL N.º 01744/2000-CR. Elaboración propia. 610
Diagrama 30. Estructura del delito de acceso ilícito y sabotaje informático (alteración, daño y destrucción), propuesto en el PL N.º 01744/2000-CR. Elaboración propia 610
Diagrama 31. Estructura del delito de inserción de enlaces maliciosos en páginas legítimas, propuesto en el PL N.º 7197/2003-CR. Elaboración propia 615
Diagrama 32. Estructura del delito de daños informáticos, propuesto en el PL N.º 10079/2003-CR. Elaboración propia. 619
Diagrama 33. Estructura del delito de intrusismo indebido a los sistemas informáticos, propuesto en el PL N.º 10079/2003-CR. Elaboración propia. 620
Diagrama 34. Estructura del delito de ingreso indebido, propuesto en el PL N.º 11346/2004-CR. Elaboración propia. 622
Diagrama 35. Estructura del delito de divulgación o utilización fraudulenta de datos, propuesto en el PL N.º 11346/2004-CR. Elaboración propia. 622
Diagrama 36. Estructura del delito de intrusión indebida, propuesto en el PL N.º 11346/2004-CR. Elaboración propia. 623
Diagrama 37. Estructura del delito de acceso indebido, propuesto en el PL N.º 1318/2006-CR. Elaboración propia. 628
Diagrama 38. Estructura del delito de sabotaje o daños a sistemas, propuesto en el PL N.º 1318/2006-CR. Elaboración propia 629
Diagrama 39. Estructura del delito de posesión de equipos o prestación de servicios de sabotaje, propuesto en el PL N.º 1318/2006-CR. Elaboración propia 630

Diagrama 40. Estructura del delito de acceso ilícito, propuesto en el PL N.º 1828/2007-CR. Elaboración propia. 638
Diagrama 41. Estructura del delito de manipulación del sistema de datos informáticos, propuesto en el PL N.º 1828/2007-CR. Elaboración propia. 638
Diagrama 42. Estructura del delito de intrusismo informático, propuesto en el PL N.º 34/2011-CR. Elaboración propia. 648
Diagrama 43. Estructura del delito de sabotaje informático, propuesto en el PL N.º 34/2011-CR. Elaboración propia. 649
Diagrama 44. Estructura del delito de prestación de equipos y servicios con fines de intrusismo y/o sabotaje, propuesto en el PL N.º 34/2011-CR. Elaboración propia. 650
Diagrama 45. Estructura del delito de espionaje informático, propuesto en el PL N.º 34/2011-CR. Elaboración propia. 650
Diagrama 46. Estructura del delito de comercialización o difusión de base de datos, propuesto en el PL N.º 307/2011-CR. Elaboración propia 653
Diagrama 47. Estructura del delito de venta ilegal de base de datos y datos personales de usuarios y consumidores, propuesto en el PL N.º 2129/2012-CR. Elaboración propia 659

V. ÍNDICE DE ESQUEMAS E IMÁGENES

ESQUEMAS

Esquema 1. Etapas de un *penetration test*. 347
Esquema 2. Análisis de la actividad del actor de amenazas Matrix en GitHub, adaptado del gráfico inicialmente elaborado por Aqua Security. 458
Esquema 3. Ciberataques dirigidos contra Ucrania, empleando *wipers* de enero de 2022 a enero de 2023. 461
Esquema 4. Pasos del ciberataque Stuxnet que dañó 1000 centrifugadoras de una central nuclear iraní. 463
Esquema 5. Pasos y etapas de una cadena de ataque contra un sistema informático. 474
Esquema 6. Puesta en marcha y explotación del *ransomware*, descrito en la Sentencia N.º 14/16 del 3 de marzo de 2016. 482

IMÁGENES

Imagen 1. Esquema o sketch del ARPA Network, 1969. 43
Imagen 2. ARPANET, 1977. 44
Imagen 3. El grupo Anonymous hackeó diversas páginas gubernamentales y pidió a sus seguidores a unirse al movimiento #OpIndependencia. 74
Imagen 4. Comparación de la cuenta original de la congresista Tania Ramírez García con la cuenta parodia o posiblemente suplantadora de identidad. 83
Imagen 5. Captura de pantalla de la plataforma alojada en la *dark web*. En ella, el grupo Qilin se adjudicó el ataque e informó sus alcances y demanda. 89

Imagen 6. En Perú, Hiperderecho y la Liga Juvenil de Defensa de Internet impulsó un proyecto muy interesante sobre el *sexting* y las medidas de seguridad que deberían adoptarse. 94
Imagen 7. Correo electrónico dirigido a la víctima, cuyo asunto es Iloveyou y al que se adjunta el gusano. 170
Imagen 8. El proyecto *Tecnoresistencias* es un espacio seguro para informarse adecuadamente y luchar contra la violencia de género en línea. 216
Imagen 9. El *ransomware* LockBit 3.0 encripta archivos, les cambia de nombre y varía el fondo de pantalla de la víctima. Entre mayo y agosto del 2023, infectó más de 60 millones de dispositivos. 248
Imagen 10. Las series y películas no solo refuerzan estereotipos sobre la figura del hacker, sino que también lo asocian frecuentemente con la comisión de delitos informáticos. 263
Imagen 11. En diversos foros, el acto de amenaza informó que contaba con casi tres millones de registros de Amazon, entre otras empresas. 319
Imagen 12. Página principal del proyecto *Have I been pwned?* 337
Imagen 13. El *Google Titan Security Key* es un *token* de seguridad que permite añadir una capa de protección a los dispositivos. 344
Imagen 14. MSpy es una aplicación de control parental cuyas funciones son invasivas. 349
Imagen 15. Página web de la municipalidad distrital de Ate, luego del *defacement attack*. 398
Imagen 16. Página web de la municipalidad de Pucusana, luego del *defacement attack*. 399
Imagen 17. Vista de una carpeta cuyos archivos fueron encriptados por el *ransomware Vovalex*. 404
Imagen 18. El procesamiento de Joaquín Sorianello puso los reflectores sobre la vulnerabilidad de los sistemas de voto electrónico del gobierno de la Ciudad de Buenos Aires. 408
Imagen 19. La página web del ex fiscal de Tabasco fue intervenida por Anonymous. 413
Imagen 20. Nota de rescate obtenida de Sentinel One. 423
Imagen 21. Último tuit publicado en la cuenta de la Biblioteca Nacional del Perú, el 22 de noviembre de 2024. 436
Imagen 22. Mensajes de ataque posteados en el canal de Telegram de *Dark Storm Team*. 438
Imagen 23. El USB Killer es vendido en diversas plataformas, entre ellas, Amazon. 454
Imagen 24. Poster difundido por el FBI contra la ciberorganización criminal REvil Sodinokibi. 481
Imagen 25. Los ciberdelincuentes de la organización *CloAk Ransomware* dieron a conocer su ataque con esta ilustración. 483
Imagen 26. Amnistía Internacional ha cuestionado la comercialización de *softwares* espías como Pegasus. 491
Imagen 27. Anuncio publicado por el FBI en el que se alertaba sobre el uso de *keylogger*. 522
Imagen 28. Anuncio publicado por el FBI en el que se alertaba sobre siete ciudadanos implicados en diversos ciberataques. 527
Imagen 29. Correo electrónico para la distribución del *malware* a través del archivo adjunto en formato de documento. 533
Imagen 30. "Este *website* ha sido ocupado; Operación *Talent*". 543
Imagen 31. Publicación obtenida en la red social X que reflejaría un posible ataque cibernético a la Corte Superior de Justicia de Arequipa. 573
Imagen 32. El cable USB-C OMG existe y ha podido ser analizado gracias a tomografías computarizadas en 3D. 576



El Observatorio Peruano de Cibercriminalidad es una asociación civil fundada el 7 de julio del 2020. Sus actividades giran alrededor de cuatro componentes fundamentales: (i) la investigación de la ciberdelincuencia, (ii) la capacitación de operadores jurídicos y de la sociedad civil, (iii) la elaboración y difusión de publicaciones digitales, y (iv) la asesoría y litigio ad honorem a favor de víctimas de este moderno fenómeno delictivo.

Como parte de sus actividades de capacitación académica, el Observatorio ha organizado los siguientes eventos:

- I Conversatorio "Audiencias Virtuales", impartido por Daniela Dupuy, Sebastián Soltau y Ricardo Elías: 2 de julio del 2020.
- II Conversatorio "Fraudes Virtuales", impartido por Sabrina Lamperti, Rafael García Borda y Ricardo Elías: 5 de agosto del 2020.
- III Conversatorio "Child Grooming", impartido por Agostina Miquelarena, Beatriz Rodríguez y Ricardo Elías: 24 de setiembre del 2020.
- La Mesa de Trabajo sobre Cibercrimen y Prueba Digital, dirigida a integrantes del Distrito Judicial de Lima Sur e impartido por Ricardo Elías: 21, 23 y 27 de julio del 2020.
- I Workshop de Litigación Oral en Entornos Virtuales, impartido por Diana González y Ricardo Elías: 4 de agosto del 2020.
- II Workshop de Litigación Oral en Entornos Virtuales, impartido por Olga del Carpio y Ricardo Elías: 12 de agosto del 2020.
- III Workshop de Litigación Oral en Entornos Virtuales, impartido por Claudia Izumi Chaco: 19 de agosto del 2020.
- Conferencia "¿Cómo garantizar el derecho de protesta? Conoce tus derechos", con la participación de Luciano López Flores, Ana Celia Hernández, Marieliv Flores y Ricardo Elías Puelles: 11 de noviembre del 2020.
- Conferencia "Aspectos generales de la ciberdelincuencia", a cargo de Ricardo Elías: 5 de enero del 2023.

- Conferencia "Problemas específicos de la tipificación: ¿cómo investigar el cibercrimen?", a cargo de Yesica Valverde Serrano: 6 de enero del 2023.
- Conferencia "Problemas específicos de la tipificación: ¿cómo investigar el cibercrimen? II", a cargo de Martín Cárdenas Castillo: 7 de enero del 2023.
- Capacitación interna "Uso de herramientas tecnológicas en la investigación Criminal", a cargo de Rafael García Borda: 26 de febrero del 2021.
- Capacitación interna "La labor de la investigación y el aseguramiento de la prueba en la era digital", a cargo de Agostina Miquelarena: 25 de marzo del 2021.
- Capacitación interna "Levantamiento del secreto de las comunicaciones en la investigación de los delitos informáticos", a cargo de Víctor Espinoza: 26 de abril del 2021.
- Capacitación interna Seguridad Digital y Privacidad, a cargo de Edgar Huaranga: 26 de abril del 2021.
- Capacitación interna "Ciberacoso en niños, niñas y adolescentes: ¿cómo aproximarnos a las víctimas?", a cargo de Marcela Scarafia y Rocío Calvo: 29 de abril del 2021.
- Capacitación interna "Criptomonedas: ¿activos digitales que aportan a la cibercriminalidad?", a cargo de Dévika Pérez: 25 de mayo del 2021.
- Capacitación interna "Introducción a la inteligencia artificial y su influencia en el derecho", a cargo de Federica Morici: 28 de mayo del 2021.
- Curso de especialización "Cibercrimen y prueba digital. Análisis de la legislación penal y procesal penal peruana", impartido por Vitor de Paula, Daniela Dupuy, Marcos Salt, Mariana Kiefer, Fernanda Gómez, Jorge L. Litvin, Dévika Pérez, Gustavo Sain, Sabrina Lamperti, Rafael García Borda, Gustavo Presman, Agostina Miquelarena, Juan Carlos Ortiz Pradillo, Julio César Tapia, Víctor Espinoza, Marlon Luna y Ricardo Elías: desde el 1 de marzo al 7 de mayo del 2022.
- Seminario Ciberdelitos contra el Patrimonio, con la participación de Ricardo Elías y Dévika Pérez: 8, 15, 22 y 24 de junio del 2023.
- Seminario "Ciberdelitos contra la disponibilidad, integridad y confidencialidad", con la participación de Ricardo Elías y Mónica Bustamante: 6, 13, 20 y 22 de julio del 2023.

- Seminario "Ciberdelitos contra la libertad y la indemnidad sexual", con la participación de Ricardo Elías y Agostina Miquelarena: 3, 10, 17 y 26 de agosto del 2023.
- Seminario Ciberdelitos e Investigación Criminal, con la participación de Ricardo Elías y Emma Calderón: 7, 14 y 28 de setiembre del 2023.
- Congreso Online "10 años de la Ley de Delitos Informáticos", con la participación de José Neyra Flores, Gustavo Sain, Martín Gershanik, Paola Charaja, Juan Carlos Ortiz Pradillo, Fátima Toche, Wendy Requejo, Julio César Tapia, María Esther Felices, Gustavo Ubiria, Gerardo Lamas, Víctor Díaz, Daniela Dupuy, Silvina Santangelo, Roberto Vílchez, Víctor Espinoza, Maguín Arévalo, Carlos Guerrero, Fiorella Chinchay y Ricardo Elías: 20, 21 y 22 de octubre del 2023.

Desde el primer día, el Observatorio asumió el firme compromiso de combatir la ciberdelincuencia con determinación y justicia. La tecnología debe ser una herramienta de progreso, no un medio para el abuso, por lo que el Observatorio ha defendido incansablemente a víctimas de suplantación de identidad, acoso virtual, grooming, acceso ilícito y fraude informático, entre otros delitos. A través de labor pro bono, no solo se brinda apoyo legal, sino que también se envía un mensaje claro: nadie está solo en esta lucha. El Observatorio seguirá alzando la voz y usando el derecho como escudo para proteger a quienes más lo necesitan.

Publicado: julio 2025
Este libro se terminó de imprimir
en julio del 2025 en los
talleres gráficos de
Pacífico Editores SAC
Jr. Castrovirreyna N.º 224 - Breña
Central: 619-3728
Lima-Perú