REPORTE TEMÁTICO N° 182/2024-2025-ASISP/DIP

Delitos informáticos
Legislación comparada

Lima, 3 de junio de 2025

PRESENTACIÓN

El Departamento de Investigación Parlamentaria, a través del Área de Servicios de Investigación y Seguimiento Presupuestal, ha elaborado el Reporte Temático N° 182 /2024-2025-ASISP/DIP, referido al ordenamiento jurídico vigente sobre los delitos informáticos en: Argentina, Bolivia, Colombia, Costa Rica, Chile, Ecuador, El Salvador y Uruguay.

Para la elaboración se ha consultado la información disponible en fuentes oficiales sobre la materia; cuyas referencias se consignan en el documento.

Esperamos brindar información que contribuya a la labor parlamentaria

I. Alcances generales

1. El Ministerio de Justicia de la República Argentina, menciona los conceptos y formas del ciberdelito[1]:

> Son conductas ilegales realizadas por ciberdelincuentes en el ciberespacio a través de dispositivos electrónicos y redes informáticas.
>
> Consiste en estafas, robos de datos personales, de información comercial estratégica, suplantación de identidad, fraudes informáticos, ataques como *cyberbulling*, *grooming*, *phishing* cometidos por ciberdelincuentes que actúan en grupos o trabajan solos.
>
> *¿Qué es el ciberespacio?*
> Es un área intangible a la que cualquier persona puede acceder con una computadora desde su hogar, su lugar de trabajo o dispositivos móviles.
>
> *¿Qué medios usan los ciberdelincuentes para cometer un ciberdelito?*
> Usan medios tecnológicos como: internet, computadoras, celulares, redes de comunicación 3G, 4G y 5G, redes de fibra óptica y *software*.
>
> *¿Cómo es más probable que se tope con el ciberdelito un usuario cotidiano de equipos y dispositivos móviles?*
> El ciberdelito puede llegar de muchas maneras: sitios web no seguros, redes sociales, agujeros creados por vulnerabilidades de seguridad, contraseñas poco seguras en cuentas y dispositivos inteligentes y, sobre todo, el correo electrónico.
>
> *¿Cuáles son los ciberdelitos y contravenciones más comunes?*
> Los ciberdelitos se cometen a través de programas maliciosos desarrollados para borrar, dañar, deteriorar, hacer inaccesibles, alterar o suprimir datos informáticos sin tu autorización y con fines económicos y de daño.
>
> Algunos ejemplos son:
>
> - **Ataques en tu navegación:** desvían tu navegador hacia páginas que causan infecciones con programas malignos como virus, gusanos y troyanos. Estos programas pueden borrar tu sistema operativo, infectar tu teléfono y tu computadora, activar tu webcam, extraer datos, etc.
> - **Ataques a servidores:** pueden dañar o robar tus datos y negarte el acceso a tu información.
> - **Corrupción de bases de datos**: interfieren en bases de datos públicas o privadas para generar datos falsos o robar información.
> - **Virus informáticos:** encriptan archivos, bloquean cerraduras inteligentes, roban dinero desde los celulares con mensajes de texto que parecen de la compañía.
> - **Programa espía:** alguno de los dispositivos tiene instalado un *software* que le permite encender y grabar con la cámara y el micrófono. También puede acceder a tu información personal sin autorización y sin que lo sepas.
>
> Los ciberdelitos usan la ingeniería social para engañarte, amenazarte y sacarte datos personales o información de otras personas u organizaciones, obtener dinero, suplantar tu identidad, acosarte digital y sexualmente.
>
> Algunos ejemplos son:
>
> - ***Phishing*** o ***vishing:*** los ciberdelincuentes se hacen pasar por empresas de servicios, oficinas de gobierno o amigos de algún familiar y te piden los datos
>
>   que les faltan para suplantar tu identidad y así operar tus cuentas en bancos, perfiles en las plataformas y redes sociales, servicios y aplicaciones web.

[1] https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/que-es-el-ciberdelito

- ***Ciberbullying:*** es el acoso por mensajería instantánea, *stalking* en WhatsApp, Telegram, Facebook Messenger y en las redes sociales con la intención de perseguir, acechar, difamar y atentar contra el honor e integridad moral de una persona. Esto lo hacen a través del descubrimiento y revelación de secretos, de la publicación de comentarios o videos ofensivos o discriminatorios, de la creación de memes o el etiquetado de tus publicaciones.

- ***Grooming:*** se trata de personas adultas que, de manera velada, intentan obtener fotografías o videos sexuales de personas menores para posteriores chantajes o previo al abuso sexual.

- **Sextorsión:** consiste en pedir dinero a cambio de no difundir en las redes imágenes generadas para un intercambio erótico consentido.

- **Ciberodio:** son contenidos inapropiados que pueden vulnerar a las personas. Se considera ciberodio a la violencia, mensajes que incitan al odio, la xenofobia, el racismo y la discriminación o el maltrato animal.

- **Pornografía infantil:** se trata de la corrupción de personas menores y su explotación sexual para producir, comercializar imágenes y videos de actividad sexual explícita.

Uso de la **inteligencia artificial** en ciberdelitos
Los ciberdelincuentes utilizan la IA para hacer sus ataques más sofisticados y difíciles de detectar. Algunas de las formas de amenazas más frecuentes son :

Phishing **personalizado:** la IA analiza datos de redes sociales para crear correos electrónicos de phishing muy convincentes, dirigidos a individuos específicos.

***Deepfakes* y suplantación de identidad:** Los deepfakes son vídeos, imágenes o archivos de voz manipulados con software de inteligencia artificial (IA) para parecer reales y auténticos. Los ciberdelincuentes pueden usarlos para extorsionar, cometer fraude o manipular a las víctimas para que realicen acciones perjudiciales.

Malware Inteligente: el malware impulsado por IA puede adaptarse y evitar ser detectado por los sistemas de seguridad tradicionales.

Exploración de Vulnerabilidades: la IA puede detectar rápidamente fallos en el software y las redes, que los atacantes pueden explotar antes de que se solucionen.

Otra dimensión del ciberdelito tiene que ver con la violación de la privacidad de las personas

- Espionaje ilícito sobre las comunicaciones privadas de los ciudadanos.

- Violación a la intimidad por parte de las empresas proveedoras de servicios de internet sin el consentimiento del usuario, para conocer sus gustos y preferencias y establecer la venta agresiva de productos y servicios asociados.

- Acceso ilegal a las comunicaciones privadas de un trabajador (correos electrónicos, redes sociales, etc.)

2. La Organización International de Policía Criminal (INTERPOL) describe el fenómeno de la ciberdelincuencia y lo clasifica en los términos siguientes[2]:

> Hoy en día, el mundo está más conectado digitalmente que nunca. Los delincuentes se están aprovechando de esta transformación en línea para atacar, a través de sus puntos débiles, las redes, infraestructuras y sistemas informáticos. Esto tiene una enorme repercusión económica y social en todo el mundo, tanto para los gobiernos, como para las empresas o los particulares.
>
> El phishing, el ransomware y las violaciones de la seguridad de los datos son solo algunos ejemplos de las actuales ciberamenazas, eso sin contar que continuamente están surgiendo nuevos tipos de ciberdelitos. Los ciberdelincuentes son cada vez más ágiles y están mejor organizados, como demuestra la velocidad con que explotan las nuevas tecnologías, y el modo en que adaptan sus ataques y cooperan entre sí de forma novedosa.
>
> Los ciberdelitos no conocen fronteras. Los delincuentes, las víctimas y las infraestructuras técnicas están dispersos por múltiples jurisdicciones, lo que resulta muy problemático a la hora de realizar una investigación o emprender acciones judiciales.
>
> (…)

3. El Proyecto #CREW, financiado con el apoyo de la Comisión Europea, brinda una definición de piratería y extorsión cibernética[3]:

> La piratería (“Hacking”) es un intento de explotar un sistema informático o una red privada dentro de un ordenador. En pocas palabras, es el acceso no autorizado o el control de los sistemas de seguridad de la red informática para algún propósito ilícito.
>
> La extorsión cibernética es un delito en Internet en el que alguien retiene archivos electrónicos o los datos de su empresa como rehenes hasta que se les pague el rescate exigido.

[2] https://www.interpol.int/es/Delitos/Ciberdelincuencia

[3] https://crewproject.eu/hacking-y-extorsion-cibernetica/

CUADRO 1

País	Delitos informáticos tipificados en el Código Penal
Argentina	• Art. 131, delito contra la integridad sexual, será penado toda persona que, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contacte a un menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual. • Art. 153, aacceso indebido a comunicaciones electrónicas, telecomunicaciones o de otra naturaleza, que esté dirigido a persona ajena y que provenga de cualquier sistema de carácter privado o de acceso restringido. • Art.155, posesión de comunicación electrónica o de otra naturaleza, no destinados a la publicidad y su publicación indebida, causando perjuicios a terceros. • Art. 157 bis, violación de sistemas de confidencialidad y seguridad de datos, acceso a un banco de datos personales, proporcionar y revelar la información registrada, insertar datos en un archivo de datos personales y si el autor es funcionario público, sufrirá, además, pena de inhabilitación. • Art. 173, uso de tarjetas de compra, crédito o débito, falsificación, adulteración, hurto, robo, perdida u obtención del legítimo emisor mediante ardid o engaño, o mediante el uso no autorizado de sus datos. • Defraudación y manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos. • Art. 183, destrucción, inutilización o desaparición de datos, documentos, programas o sistemas informáticos; venta, distribución, hacer circular o introducir en un sistema informático, cualquier programa destinado a causar daños. • Art. 184**,** ejecución de daños en archivos, registros, datos, documentos, programas o sistemas informáticos públicos; en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público. • Art. 197, interrupción o entorpecimiento de la comunicación telegráfica, telefónica o de otra naturaleza o resistencia violenta en el restablecimiento de la comunicación interrumpida. • Art. 255, sustracción, alteración, ocultamiento, destrucción o inutilización en todo o en parte de objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario público o de otra persona en el interés del servicio público.
Bolivia	• Art. 363 bis, (manipulación informática) manipulación de procesamientos o transferencia de datos informáticos que conduzca a un resultado, ocasionando una transferencia patrimonial en perjuicio de terceros.

	• Art. 363 ter, (alteración, acceso y uso indebido de datos informáticos) acceso, utilización, modificación, supresión o inutilización de datos almacenados en una computadora o en cualquier soporte informático, ocasionando perjuicio.
Colombia	• Art. 269A. Acceso abusivo a un sistema informático. Acceso en todo o en parte a un sistema informático sin autorización. • Art. 269B.Obstaculización ilegítima de sistema informático o red de telecomunicación. Obstaculización del funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones. • Art. 269C.Interceptación de datos informáticos. Interceptación de datos informáticos de un sistema informático, o las emisiones electromagnéticas sin orden judicial. • Art. 269D. *Daño Informático*. Destrucción, daño, eliminación, deterioro, alteración o supresión de datos informáticos, o de un sistema de tratamiento de información. • Art. 269E. *Uso de software malicioso*. Producción, tráfico, adquisición, distribución, venta, envío, introducción o extracción del territorio nacional software malicioso u otros programas de computación de efectos dañinos. • Art. 269F. *Violación de datos personales*. Obtención, compilación, sustracción, ofrecimiento, venta, intercambio, envío, compra, obstrucción, divulgación, modificación o empleo de códigos en datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes. • Art. 269G. *Suplantación de sitios web para capturar datos personales*. Diseño, desarrollo, tráfico, venta, ejecución, programación o envío de páginas electrónicas, enlaces o ventanas emergentes; modificación del sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente. • Art. 269H. *Circunstancias de agravación punitiva*: ▪ Si los delitos se cometen en redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros. ▪ Por servidor público en ejercicio de sus funciones. ▪ Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este. ▪ Revelando o dando a conocer el contenido de la información en perjuicio de otro. ▪ Obteniendo provecho para sí o para un tercero. ▪ Con fines terroristas o generando riesgo para la seguridad o defensa nacional. ▪ Utilizando como instrumento a un tercero de buena fe. ▪ Si es el responsable de la administración, manejo o control de dicha información. • Art. 269I. Hurto por medios informáticos y semejantes. Manipulación de un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos.

	• Art. 269J.Transferencia no consentida de activos. Transferencia no consentida de cualquier activo en perjuicio de un tercero.
Costa rica	• Art. 167. Corrupción. Corrupción de una persona menor de edad o incapaz, con fines eróticos, pornográficos u obscenos, en exhibiciones o espectáculos públicos o privados, aunque la persona menor de edad o incapaz lo consienta. • Utilización de las redes sociales o cualquier otro medio informático o telemático, u otro medio de comunicación, para buscar encuentros de carácter sexual para sí, para otro o para grupos, con una persona menor de edad o incapaz; utiliza a estas personas para promover la corrupción o las obliga o instiga a realizar actos sexuales, prematuros, aunque la victima consienta participar en ellos o verlos ejecutar. • Art. 167 bis. Seducción o encuentros con persona menor de edad o incapaz por medios electrónicos. Suplantación o uso de identidad falsa, por cualquier medio para establecer comunicaciones de contenido sexual o erótico, ya sea que se incluyan o no imágenes, videos, textos o audios, con una persona menor de edad o incapaz. • Art. 196. Violación de correspondencia o comunicaciones. Acceso, modificación, alteración, destrucción, intervención, interceptación, entrega, venta, remisión o desvío de su destino documentación o comunicaciones dirigidas a otra persona. • Art. 196 bis. Violación de datos personales. Apoderamiento, modificación, interferencia, acceso, copia, transmisión, publicación, difusión, recopilación, inutilización, interceptación, retención, venta, compra, desvío 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. • Art. 214. Extorsión**.** El que procure un lucro y obligue a otro, con intimidación o con amenazas graves, a tomar una disposición patrimonial perjudicial para sí mismo o para un tercero. • Art. 217 bis. Estafa informática. El en perjuicio de una persona física o jurídica, manipule o influya en el ingreso, en el procesamiento o en el resultado de los datos de un sistema automatizado de información, ya sea mediante el uso de datos falsos o incompletos, el uso indebido de datos, programación, valiéndose de alguna operación informática o artificio tecnológico, o bien, por cualquier otra acción que incida en el procesamiento de los datos del sistema o que dé como resultado información falsa, incompleta o fraudulenta, con la cual procure u obtenga un beneficio patrimonial o indebido para sí o para otro. • Art. 229. Daño agravado. Cuando el daño recayera sobre redes, sistemas o equipos informáticos, telemáticos o electrónicos, o sus componentes físicos, lógicos o periféricos. • Art. 229 bis. Daño informático. 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. • Art. 229 ter. Sabotaje informático. 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.

	• Art. 230. Suplantación de identidad. Quien suplante la identidad de una persona física, jurídica o de una marca comercial en cualquiera red social, sitio de Internet, medio electrónico o tecnológico de información. • Art. 231. Espionaje informático. Sin autorización del titular o responsable, valiéndose de cualquier manipulación informática o tecnológica, se apodere, transmita, copie, modifique, destruya, utilice, bloquee o recicle información de valor para el tráfico económico de la industria y el comercio. • Art. 232. Instalación o propagación de programas informáticos maliciosos. 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. • Art. 233. Suplantación de páginas electrónicas. En perjuicio de un tercero, suplante sitios legítimos de la red de Internet. • Art. Facilitación del delito informático. quien facilite los medios para la consecución de un delito efectuado mediante un sistema o red informática o telemática, o los contenedores electrónicos, ópticos o magnéticos. • Art. 235. Narcotráfico y crimen organizado. Cualquiera de los delitos cometidos por medio de un sistema o red informática o telemática, o los contenedores electrónicos, ópticos o magnéticos afecte la lucha contra el narcotráfico o el crimen organizado. • Art. 236. Difusión de información falsa. Quien, a través de medios electrónicos, informáticos, o mediante un sistema de telecomunicaciones, propague o difunda noticias o hechos falsos capaces de distorsionar o causar perjuicio a la seguridad y estabilidad del sistema financiero o de sus usuarios.
Chile	• La Ley 21459[4] establece normas sobre delitos informáticos, derogando la Ley 19.223 y adecuándose al Convenio de Budapest.
Ecuador	• Art. 230. Interceptación ilegal de datos. ▪ Quien, sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible. ▪ Quien diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder. ▪ A través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares.

[4] Chile. Ley 21459. Establece normas sobre delitos informáticos, deroga la Ley 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest. Ver texto de la norma: https://www.bcn.cl/leychile/navegar?idNorma=1177743

	▪ Quien produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior. • Art. 231. Transferencia electrónica de activo patrimonial. Quien, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para la apropiación no consentida de un activo patrimonial de otra persona. • Art. 232.- Ataque a la integridad de sistemas informáticos. • Quien destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen. • Quien diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo. • Quien destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general. • Art. 234. Acceso no consentido a un sistema informático, telemático o de telecomunicaciones. Quien sin autorización acceda en 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, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años.
El Salvador	• Los delitos informáticos están tipificados en el Decreto 260. Ley Especial contra los Delitos Informáticos y Conexos[5].
Perú	• La Ley 30096[6] sanciona las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, y deroga los artículos 207-A al 207-C del Capítulo X sobre Delitos Informáticos del código Penal.
Uruguay	• Art. 288 BIS. (Acoso telemático). - Mediante la utilización de medios telemáticos, desarrolle de forma insistente cualquiera de las siguientes conductas: vigilar, perseguir o procurar cercanía física, estableciendo o intentando establecer contacto con una persona, sea de forma directa o por intermedio de terceros, de tal modo que altere gravemente el desarrollo de su vida.

[5] Decreto 260. Ley Especial contra los Delitos Informáticos y Conexos. Ver texto de la norma: Microsoft Word - LEY ESPECIAL CONTRA LOS DELITOS INFORMATICOS Y CONEXOS 01

[6] Ley 30096, Ley de Delitos Informáticos. Ver: https://spij.minjus.gob.pe/spij-ext-web/#/detallenorma/H1088463

	• Art. 288 TER. (Circunstancias agravantes especiales del delito de acoso telemático). En detrimento de un menor de edad, de adultos incapaces, de personas que previamente hayan tenido una relación afectiva o íntima, o de individuos vulnerables por enfermedad o por situaciones especiales que supongan una mayor fragilidad. • Art. 347 BIS. (Fraude informático). Inducir, con estratagemas o engaños artificiosos, incite en error a alguna persona para obtener información mediante tecnologías de la información y de la comunicación. Efectuar manipulaciones informáticas o artificios afines con el fin de realizar operaciones financieras, transferencias o pagos no consentidos. Utilizar cualquier tipo de tarjeta, cheque, código o cualquier otro medio de pago, o los datos vinculados a los mismos, para realizar transferencias, pagos o cualquier operación no consentida. • Art. 348 BIS. (Circunstancias agravantes). Que exista parentesco o vinculación laboral o afectiva con la víctima o el tercero perjudicado. Que el hecho se efectúe en perjuicio del Estado o de cualquier ente público, o afecte infraestructuras críticas. Que el hecho se efectúe generando en la víctima el temor de un peligro imaginario o la persuasión de obedecer a una orden de la autoridad. • Art. 358 QUATER. (Daño informático). El que, por cualquier medio y sin autorización, destruya, altere o inutilice datos o sistemas informáticos con la finalidad de causar daño. • Art. 359 TER. - Serán circunstancias agravantes especiales del delito de daño informático: Que el daño ocasionado sea irreparable o sea imposible retornar a su estado anterior. Que el daño se cometa en perjuicio de documentos electrónicos o sistemas informáticos de carácter estatal o vinculados a infraestructuras críticas. • Art. 297 BIS. (Acceso ilícito a datos informáticos). El que, mediante medios informáticos o telemáticos, sin autorización y sin justa causa acceda, interfiera, difunda, venda o ceda información ajena contenida en soporte digital. • Art. 297 TER. (Interceptación ilícita). El que sin autorización y sin justa causa intercepte, interrumpa o interfiera por medios técnicos, datos informáticos en transmisiones no públicas, dirigidas a un sistema informático, sean originadas en un sistema informático o efectuadas dentro del mismo, incluyendo las emisiones electromagnéticas provenientes de un sistema informático que transporte los mismos. • Art. 297 QUATER. (Vulneración de datos). El que mediante la utilización de cualquier medio telemático acceda, se apodere, utilice, o modifique datos confidenciales de terceros, registrados en soportes digitales, o cualquier otro tipo de archivo o registro público o privado, sin autorización de su titular. • Art. 347 TER. (Suplantación de identidad). El que usurpe, adopte, cree o se apropie de la identidad de otra persona física o jurídica, valiéndose de cualquier medio, herramienta tecnológica o sistema informático, obteniendo datos accediendo a redes sociales, casillas de correo electrónico, cuentas bancarias, medios de pago, plataformas digitales, o cualquier credencial digital o factor de autenticación, con la intención de dañar a su legítimo titular.

	• No constituirá suplantación de identidad la creación de nuevos perfiles destinados exclusivamente a la parodia. • Art. 348 TER. (Circunstancias agravantes especiales). Serán circunstancias agravantes especiales del delito de suplantación de identidad: ▪ Que se cometa con la finalidad de divulgar la información a la cual se accedió. ▪ Que se modifiquen, supriman o adulteren datos de la víctima o utilicen las credenciales para vincularse con terceras personas físicas o jurídicas. ▪ Que se adquieran, mediante el uso indebido de sus datos personales productos o mercaderías, o contraten servicios a través de medios telemáticos, en nombre de la víctima. ▪ Que se suplante la identidad de un organismo estatal u otro vinculado a infraestructuras críticas. ▪ La concurrencia con extorsión a la víctima, sus familiares o terceras personas vinculadas, para la obtención de activos o cualquier prestación en especie a los efectos de recuperar las referidas credenciales. • Art. 358 QUINQUIES. (Abuso de los dispositivos). El que, de forma ilegítima, produzca, adquiera, importe, comercialice o facilite a terceros, programas, sistemas informáticos o telemáticos de cualquier índole, credenciales o contraseñas de acceso a datos informáticos o sistemas de información, destinados inequívocamente a la comisión de un delito.

Fuente: Códigos Penales. Elaboración: Área de Servicios de Información y Seguimiento Presupuestal (ASISP)

CUADRO 2

LEGISLACIÓN SOBRE DELITOS INFORMÁTICOS EN ARGENTINA, BOLIVIA, COLOMBIA, COSTA RICA, CHILE, ECUADOR, EL SALVADOR Y URUGUAY

País	Norma	Artículo
Argentina	Constitución de la Nación	**Artículo 43.-** Toda persona puede interponer acción expedita y rápida de amparo, siempre que no exista otro medio judicial más idóneo, contra todo acto u omisión de autoridades públicas o de particulares, que en forma actual o inminente lesione, restrinja, altere o amenace, con arbitrariedad o ilegalidad manifiesta, derechos y garantías reconocidos por esta Constitución, un tratado o una ley. En el caso, el juez podrá declarar la inconstitucionalidad de la norma en que se funde el acto u omisión lesiva. Podrán interponer esta acción contra cualquier forma de discriminación y en lo relativo a los derechos que protegen al ambiente, a la competencia, al usuario y al consumidor, así como a los derechos de incidencia colectiva en general, el afectado, el defensor del pueblo y las asociaciones que propendan a esos fines, registradas conforme a la ley, la que determinará los requisitos y formas de su organización. Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos. No podrá afectarse el secreto de las fuentes de información periodística. (…).
	Ley 25.326 Ley de Protección de los Datos Personales Disposiciones Generales. Principios generales relativos a la protección de datos. Derechos de los titulares de datos. Usuarios y responsables de archivos, registros y	Capítulo I Disposiciones Generales **ARTICULO 1°** — (Objeto). La presente ley tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional. Las disposiciones de la presente ley también serán aplicables, en cuanto resulte pertinente, a los datos relativos a personas de existencia ideal. En ningún caso se podrán afectar la base de datos ni las fuentes de información periodísticas. (…).

	bancos de datos. Control. Sanciones. Acción de protección de los datos personales.	Capítulo II Principios generales relativos a la protección de datos **ARTICULO 3°** — (Archivos de datos – Licitud). La formación de archivos de datos será lícita cuando se encuentren debidamente inscriptos, observando en su operación los principios que establece la presente ley y las reglamentaciones que se dicten en su consecuencia. Los archivos de datos no pueden tener finalidades contrarias a las leyes o a la moral pública. **ARTICULO 4°** — (Calidad de los datos). 1. Los datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido. 2. La recolección de datos no puede hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la presente ley. 3. Los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención. 4. Los datos deben ser exactos y actualizarse en el caso de que ello fuere necesario. 5. Los datos total o parcialmente inexactos, o que sean incompletos, deben ser suprimidos y sustituidos, o en su caso completados, por el responsable del archivo o base de datos cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate, sin perjuicio de los derechos del titular establecidos en el artículo 16 de la presente ley. 6. Los datos deben ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular. 7. Los datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados. **ARTICULO 5°** — (Consentimiento). 1. El tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su consentimiento libre, expreso e informado, el que deberá constar por escrito, o por otro medio que permita se le equipare, de acuerdo a las circunstancias. El referido consentimiento prestado con otras declaraciones, deberá figurar en forma expresa y destacada, previa notificación al requerido de datos, de la información descrita en el artículo 6° de la presente ley. 2. No será necesario el consentimiento cuando: a) Los datos se obtengan de fuentes de acceso público irrestricto; b) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal; c) Se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio; d) Deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento; e) Se trate de las operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes conforme las disposiciones del artículo 39 de la Ley 21.526. **ARTICULO 6°** — (Información). Cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa y clara:

		a) La finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o clase de destinatarios; b) La existencia del archivo, registro, banco de datos, electrónico o de cualquier otro tipo, de que se trate y la identidad y domicilio de su responsable; c) El carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga, en especial en cuanto a los datos referidos en el artículo siguiente; d) Las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos; e) La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos. (…). **ARTICULO 9°** — (Seguridad de los datos). 1. El responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado. 2. Queda prohibido registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad. **ARTICULO 10.** — (Deber de confidencialidad). 1. El responsable y las personas que intervengan en cualquier fase del tratamiento de datos personales están obligados al secreto profesional respecto de los mismos. Tal obligación subsistirá aun después de finalizada su relación con el titular del archivo de datos. 2. El obligado podrá ser relevado del deber de secreto por resolución judicial y cuando medien razones fundadas relativas a la seguridad pública, la defensa nacional o la salud pública. **ARTICULO 11.** — (Cesión). 1. Los datos personales objeto de tratamiento sólo pueden ser cedidos para el cumplimiento de los fines directamente relacionados con el interés legítimo del cedente y del cesionario y con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la cesión e identificar al cesionario o los elementos que permitan hacerlo. 2. El consentimiento para la cesión es revocable. 3. El consentimiento no es exigido cuando: a) Así lo disponga una ley; b) En los supuestos previstos en el artículo 5° inciso 2; c) Se realice entre dependencias de los órganos del Estado en forma directa, en la medida del cumplimiento de sus respectivas competencias; d) Se trate de datos personales relativos a la salud, y sea necesario por razones de salud pública, de emergencia o para la realización de estudios epidemiológicos, en tanto se preserve la identidad de los titulares de los datos mediante mecanismos de disociación adecuados; e) Se hubiera aplicado un procedimiento de disociación de la información, de modo que los titulares de los datos sean inidentificables. 4. El cesionario quedará sujeto a las mismas obligaciones legales y reglamentarias del cedente y éste responderá solidaria y conjuntamente por la observancia de las mismas ante el organismo de control y el titular de los datos de que se trate.

		ARTICULO 12. — (Transferencia internacional). 1. Es prohibida la transferencia de datos personales de cualquier tipo con países u organismos internacionales o supranacionales, que no propocionen niveles de protección adecuados. 2. La prohibición no regirá en los siguientes supuestos: a) Colaboración judicial internacional; b) Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado, o una investigación epidemiológica, en tanto se realice en los términos del inciso e) del artículo anterior; c) Transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme la legislación que les resulte aplicable; d) Cuando la transferencia se hubiera acordado en el marco de tratados internacionales en los cuales la República Argentina sea parte; e) Cuando la transferencia tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico. (…). Capítulo IV Usuarios y responsables de archivos, registros y bancos de datos **ARTICULO 21.** — (Registro de archivos de datos. Inscripción). 1. Todo archivo, registro, base o banco de datos público, y privado destinado a proporcionar informes debe inscribirse en el Registro que al efecto habilite el organismo de control. 2. El registro de archivos de datos debe comprender como mínimo la siguiente información: a) Nombre y domicilio del responsable; b) Características y finalidad del archivo; c) Naturaleza de los datos personales contenidos en cada archivo; d) Forma de recolección y actualización de datos; e) Destino de los datos y personas físicas o de existencia ideal a las que pueden ser transmitidos; f) Modo de interrelacionar la información registrada; g) Medios utilizados para garantizar la seguridad de los datos, debiendo detallar la categoría de personas con acceso al tratamiento de la información; h) Tiempo de conservación de los datos; i) Forma y condiciones en que las personas pueden acceder a los datos referidos a ellas y los procedimientos a realizar para la rectificación o actualización de los datos. 3) Ningún usuario de datos podrá poseer datos personales de naturaleza distinta a los declarados en el registro. El incumplimiento de estos requisitos dará lugar a las sanciones administrativas previstas en el capítulo VI de la presente ley. **ARTICULO 22.** — (Archivos, registros o bancos de datos públicos).

		1. Las normas sobre creación, modificación o supresión de archivos, registros o bancos de datos pertenecientes a organismos públicos deben hacerse por medio de disposición general publicada en el Boletín Oficial de la Nación o diario oficial. 2. Las disposiciones respectivas, deben indicar: a) Características y finalidad del archivo; b) Personas respecto de las cuales se pretenda obtener datos y el carácter facultativo u obligatorio de su suministro por parte de aquéllas; c) Procedimiento de obtención y actualización de los datos; d) Estructura básica del archivo, informatizado o no, y la descripción de la naturaleza de los datos personales que contendrán; e) Las cesiones, transferencias o interconexiones previstas; f) Organos responsables del archivo, precisando dependencia jerárquica en su caso; g) Las oficinas ante las que se pudiesen efectuar las reclamaciones en ejercicio de los derechos de acceso, rectificación o supresión. 3. En las disposiciones que se dicten para la supresión de los registros informatizados se esta blecerá el destino de los mismos o las medidas que se adopten para su destrucción. (…). Capítulo V Control **ARTICULO 29.** — (Organo de Control). **1. El órgano de control deberá realizar todas las acciones necesarias para el cumplimiento de los objetivos y demás disposiciones de la presente ley. A tales efectos tendrá las siguientes funciones y atribuciones:** a) Asistir y asesorar a las personas que lo requieran acerca de los alcances de la presente y de los medios legales de que disponen para la defensa de los derechos que ésta garantiza; b) Dictar las normas y reglamentaciones que se deben observar en el desarrollo de las actividades comprendidas por esta ley; c) Realizar un censo de archivos, registros o bancos de datos alcanzados por la ley y mantener el registro permanente de los mismos; d) Controlar la observancia de las normas sobre integridad y seguridad de datos por parte de los archivos, registros o bancos de datos. A tal efecto podrá solicitar autorización judicial para acceder a locales, equipos, o programas de tratamiento de datos a fin de verificar infracciones al cumplimiento de la presente ley; e) Solicitar información a las entidades públicas y privadas, las que deberán proporcionar los antecedentes, documentos, programas u otros elementos relativos al tratamiento de los datos personales que se le requieran. En estos casos, la autoridad deberá garantizar la seguridad y confidencialidad de la información y elementos suministrados; f) Imponer las sanciones administrativas que en su caso correspondan por violación a las normas de la presente ley y de las reglamentaciones que se dicten en su consecuencia; g) Constituirse en querellante en las acciones penales que se promovieran por violaciones a la presente ley; h) Controlar el cumplimiento de los requisitos y garantías que deben reunir los archivos o bancos de datos privados destinados a suministrar informes, para obtener la correspondiente inscripción en el Registro creado por esta ley.

		2. El órgano de control gozará de autonomía funcional y actuará como órgano descentralizado en el ámbito del Ministerio de Justicia y Derechos Humanos de la Nación. **3. El órgano de control será dirigido y administrado por un Director designado por el término de cuatro (4) años, por el Poder Ejecutivo con acuerdo del Senado de la Nación, debiendo ser seleccionado entre personas con antecedentes en la materia.** El Director tendrá dedicación exclusiva en su función, encontrándose alcanzado por las incompatibilidades fijadas por ley para los funcionarios públicos y podrá ser removido por el Poder Ejecutivo por mal desempeño de sus funciones. **ARTICULO 30. —** (Códigos de conducta). 1. Las asociaciones o entidades representativas de responsables o usuarios de bancos de datos de titularidad privada podrán elaborar códigos de conducta de práctica profesional, que establezcan normas para el tratamiento de datos personales que tiendan a asegurar y mejorar las condiciones de operación de los sistemas de información en función de los principios establecidos en la presente ley. 2. Dichos códigos deberán ser inscriptos en el registro que al efecto lleve el organismo de control, quien podrá denegar la inscripción cuando considere que no se ajustan a las disposiciones legales y reglamentarias sobre la materia. Capítulo VI Sanciones **ARTICULO 31. —** (Sanciones administrativas). 1. Sin perjuicio de las responsabilidades administrativas que correspondan en los casos de responsables o usuarios de bancos de datos públicos; de la responsabilidad por daños y perjuicios derivados de la inobservancia de la presente ley, y de las sanciones penales que correspondan, el organismo de control podrá aplicar las sanciones de apercibimiento, suspensión, multa de mil pesos ($ 1.000.-) a cien mil pesos ($ 100.000.-), clausura o cancelación del archivo, registro o banco de datos. 2. La reglamentación determinará las condiciones y procedimientos para la aplicación de las sanciones previstas, las que deberán graduarse en relación a la gravedad y extensión de la violación y de los perjuicios derivados de la infracción, garantizando el principio del debido proceso. **ARTICULO 32. —** (Sanciones penales). 1. Incorpórase como artículo 117 bis del Código Penal, el siguiente: "1°. Será reprimido con la pena de prisión de un mes a dos años el que insertara o hiciera insertar a sabiendas datos falsos en un archivo de datos personales. 2°. La pena será de seis meses a tres años, al que proporcionara a un tercero a sabiendas información falsa contenida en un archivo de datos personales.

		3°. La escala penal se aumentará en la mitad del mínimo y del máximo, cuando del hecho se derive perjuicio a alguna persona. 4°. Cuando el autor o responsable del ilícito sea funcionario público en ejercicio de sus funciones, se le aplicará la accesoria de inhabilitación para el desempeño de cargos públicos por el doble del tiempo que el de la condena". 2. Incorpórase como artículo 157 bis del Código Penal el siguiente: "Será reprimido con la pena de prisión de un mes a dos años el que: 1°. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales; 2°. Revelare a otro información registrada en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de una ley. Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de uno a cuatro años". Capítulo VII Acción de protección de los datos personales **ARTICULO 33. —** (Procedencia). 1. La acción de protección de los datos personales o de hábeas data procederá: a) para tomar conocimiento de los datos personales almacenados en archivos, registros o bancos de datos públicos o privados destinados a proporcionar informes, y de la finalidad de aquéllos; b) en los casos en que se presuma la falsedad, inexactitud, desactualización de la información de que se trata, o el tratamiento de datos cuyo registro se encuentra prohibido en la presente ley, para exigir su rectificación, supresión, confidencialidad o actualización. **ARTICULO 34.** — (Legitimación activa). La acción de protección de los datos personales o de hábeas data podrá ser ejercida por el afectado, sus tutores o curadores y los sucesores de las personas físicas, sean en línea directa o colateral hasta el segundo grado, por sí o por intermedio de apoderado. Cuando la acción sea ejercida por personas de existencia ideal, deberá ser interpuesta por sus representantes legales, o apoderados que éstas designen al efecto. En el proceso podrá intervenir en forma coadyuvante el Defensor del Pueblo. **ARTICULO 35. —** (Legitimación pasiva). La acción procederá respecto de los responsables y usuarios de bancos de datos públicos, y de los privados destinados a proveer informes.

		ARTICULO 36. — (Competencia). Será competente para entender en esta acción el juez del domicilio del actor; el del domicilio del demandado; el del lugar en el que el hecho o acto se exteriorice o pudiera tener efecto, a elección del actor. Procederá la competencia federal: a) cuando se interponga en contra de archivos de datos públicos de organismos nacionales, y b) cuando los archivos de datos se encuentren interconectados en redes interjurisdicciones, nacionales o internacionales. **ARTICULO 37.** — (Procedimiento aplicable). La acción de hábeas data tramitará según las disposiciones de la presente ley y por el procedimiento que corresponde a la acción de amparo común y supletoriamente por las normas del Código Procesal Civil y Comercial de la Nación, en lo atinente al juicio sumarísimo. **ARTICULO 38.** — (Requisitos de la demanda). 1. La demanda deberá interponerse por escrito, individualizando con la mayor precisión posible el nombre y domicilio del archivo, registro o banco de datos y, en su caso, el nombre del responsable o usuario del mismo. En el caso de los archivos, registros o bancos públicos, se procurará establecer el organismo estatal del cual dependen. 2. El accionante deberá alegar las razones por las cuales entiende que en el archivo, registro o banco de datos individualizado obra información referida a su persona; los motivos por los cuales considera que la información que le atañe resulta discriminatoria, falsa o inexacta y justificar que se han cumplido los recaudos que hacen al ejercicio de los derechos que le reconoce la presente ley. 3. El afectado podrá solicitar que mientras dure el procedimiento, el registro o banco de datos asiente que la información cuestionada está sometida a un proceso judicial. 4. El Juez podrá disponer el bloqueo provisional del archivo en lo referente al dato personal motivo del juicio cuando sea manifiesto el carácter discriminatorio, falso o inexacto de la información de que se trate. 5. A los efectos de requerir información al archivo, registro o banco de datos involucrado, el criterio judicial de apreciación de las circunstancias requeridas en los puntos 1 y 2 debe ser amplio. **ARTICULO 39.** — (Trámite). 1. Admitida la acción el juez requerirá al archivo, registro o banco de datos la remisión de la información concerniente al accionante. Podrá asimismo solicitar informes sobre el soporte técnico de datos, documentación de base relativa a la recolección y cualquier otro aspecto que resulte conducente a la resolución de la causa que estime procedente. 2. El plazo para contestar el informe no podrá ser mayor de cinco días hábiles, el que podrá ser ampliado prudencialmente por el juez. **ARTICULO 40.** — (Confidencialidad de la información). 1. Los registros, archivos o bancos de datos privados no podrán alegar la confidencialidad de la información que se les requiere salvo el caso en que se afecten las fuentes de información periodística.

		2. Cuando un archivo, registro o banco de datos público se oponga a la remisión del informe solicitado con invocación de las excepciones al derecho de acceso, rectificación o supresión, autorizadas por la presente ley o por una ley específica; deberá acreditar los extremos que hacen aplicable la excepción legal. En tales casos, el juez podrá tomar conocimiento personal y directo de los datos solicitados asegurando el mantenimiento de su confidencialidad. **ARTICULO 41.** — (Contestación del informe). Al contestar el informe, el archivo, registro o banco de datos deberá expresar las razones por las cuales incluyó la información cuestionada y aquellas por las que no evacuó el pedido efectuado por el interesado, de conformidad a lo establecido en los artículos 13 a 15 de la ley. **ARTICULO 42.** — (Ampliación de la demanda). Contestado el informe, el actor podrá, en el término de tres días, ampliar el objeto de la demanda solicitando la supresión, rectificación, confidencialidad o actualización de sus datos personales, en los casos que resulte procedente a tenor de la presente ley, ofreciendo en el mismo acto la prueba pertinente. De esta presentación se dará traslado al demandado por el término de tres días. **ARTICULO 43.** — (Sentencia). 1. Vencido el plazo para la contestación del informe o contestado el mismo, y en el supuesto del artículo 42, luego de contestada la ampliación, y habiendo sido producida en su caso la prueba, el juez dictará sentencia. 2. En el caso de estimarse procedente la acción, se especificará si la información debe ser suprimida, rectificada, actualizada o declarada confidencial, estableciendo un plazo para su cumplimiento. 3. El rechazo de la acción no constituye presunción respecto de la responsabilidad en que hubiera podido incurrir el demandante. 4. En cualquier caso, la sentencia deberá ser comunicada al organismo de control, que deberá llevar un registro al efecto. **ARTICULO 44.** — (Ámbito de aplicación). Las normas de la presente ley contenidas en los Capítulos I, II, III y IV, y artículo 32 son de orden público y de aplicación en lo pertinente en todo el territorio nacional. Se invita a las provincias a adherir a las normas de esta ley que fueren de aplicación exclusiva en jurisdicción nacional. La jurisdicción federal regirá respecto de los registros, archivos, bases o bancos de datos interconectados en redes de alcance interjurisdiccional, nacional o internacional. **ARTICULO 45.** — El Poder Ejecutivo Nacional deberá reglamentar la presente ley y establecer el organismo de control dentro de los ciento ochenta días de su promulgación. **ARTICULO 46.** — (Disposiciones transitorias). Los archivos, registros, bases o bancos de datos destinados a proporcionar informes, existentes al momento de la sanción de la presente ley, deberán inscribirse en el registro que se habilite conforme a lo dispuesto en el artículo 21 y adecuarse a lo que dispone el presente régimen dentro del plazo que al efecto establezca la reglamentación.

		ARTICULO 47. — Los bancos de datos prestadores de servicios de información crediticia deberán suprimir, o en su caso, omitir asentar, todo dato referido al incumplimiento o mora en el pago de una obligación, si ésta hubiere sido cancelada al momento de la entrada en vigencia de la presente ley.
	Código Penal de la Nación	**ARTICULO 131. -** Será penado con prisión de seis (6) meses a cuatro (4) años el que, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contactare a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma. **ARTICULO 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. **ARTICULO 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. **ARTICULO 154. -** Será reprimido con prisión de uno a cuatro años, el empleado de correos o telégrafos que, abusando de su empleo, se apoderare de una carta, de un pliego, de un telegrama o de otra pieza de correspondencia, se impusiere de su contenido, la entregare o comunicare a otro que no sea el destinatario, la suprimiere, la ocultare o cambiare su texto.

		ARTICULO 155. - Será reprimido con multa de pesos un mil quinientos ($ 1.500) a pesos cien mil ($ 100.000), el que hallándose en posesión de una correspondencia, una comunicación electrónica, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, no destinados a la publicidad, los hiciere publicar indebidamente, si el hecho causare o pudiere causar perjuicios a terceros. Está exento de responsabilidad penal el que hubiere obrado con el propósito inequívoco de proteger un interés público. (…). **ARTICULO 157 bis. -**Será reprimido con la pena de prisión de un (1) mes a dos (2) años el que: 1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales. 2. Ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley. 3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales. Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de un (1) a cuatro (4) años. Cuando las conductas reprimidas se hicieran para acceder, revelar, insertar o suprimir datos que afectaren a un banco de datos genéticos, registros, exámenes o muestras de ADN, la pena será de prisión de seis (6) meses a cuatro (4) años, con más inhabilitación especial para ejercer la profesión de dos (2) a cinco (5) años. (…). **ARTICULO 173.-** Sin perjuicio de la disposición general del artículo precedente, se considerarán casos especiales de defraudación y sufrirán la pena que él establece: (…); 15. El que defraudare mediante el uso de una tarjeta de compra, crédito o débito, cuando la misma hubiere sido falsificada, adulterada, hurtada, robada, perdida u obtenida del legítimo emisor mediante ardid o engaño, o mediante el uso no autorizado de sus datos, aunque lo hiciere por medio de una operación automática. 16. El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos. (…).

		ARTICULO 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 o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños. **ARTICULO 184. -** La pena será de tres (3) meses a cuatro (4) años de prisión, si mediare cualquiera de las circunstancias siguientes: (…); 5. Ejecutarlo en archivos, registros, bibliotecas, museos o en puentes, caminos, paseos u otros bienes de uso público; o en tumbas, signos conmemorativos, monumentos, estatuas, cuadros u otros objetos de arte colocados en edificios o lugares públicos; o en datos, documentos, programas o sistemas informáticos públicos; 6. Ejecutarlo en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público. (…). **ARTICULO 197.** - Será reprimido con prisión de seis (6) meses a dos (2) años, el que interrumpiere o entorpeciere la comunicación telegráfica, telefónica o de otra naturaleza o resistiere violentamente el restablecimiento de la comunicación interrumpida. (…). **ARTICULO 255.** - Será reprimido con prisión de un (1) mes a cuatro (4) años, el que sustrajere, alterare, ocultare, destruyere o inutilizare en todo o en parte objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario público o de otra persona en el interés del servicio público. Si el autor fuere el mismo depositario, sufrirá además inhabilitación especial por doble tiempo. Si el hecho se cometiere por imprudencia o negligencia del depositario, éste será reprimido con multa de pesos setecientos cincuenta ($ 750) a pesos doce mil quinientos ($ 12.500).
	Ley 27590 Ley “Mica Ortega” Programa Nacional de Prevención y Concientización del Grooming o Ciberacoso	**Artículo 1º- Créase el Programa Nacional de Prevención y Concientización del Grooming o Ciberacoso contra Niñas, Niños y Adolescentes.** **Artículo 2º-** El Programa creado en el artículo 1º tendrá como objetivo prevenir, sensibilizar y generar conciencia en la población sobre la problemática del grooming o ciberacoso a través del uso responsable de las Tecnologías de la Información y la Comunicación (TICs) y de la capacitación de la comunidad educativa en su conjunto.

	contra Niñas, Niños y Adolescentes.	**Artículo 3º-** A los fines de la presente ley se entiende por grooming o ciberacoso a la acción en la que una persona por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contacte a una persona menor de edad con el propósito de cometer cualquier delito contra la integridad sexual de la misma. **Artículo 4°-** Son objetivos del Programa Nacional de Prevención y Concientización del Grooming o Ciberacoso contra Niñas, Niños y Adolescentes: a) Generar conciencia sobre el uso responsable de las Tecnologías de la Información y Comunicación. b) Garantizar la protección de los derechos de las niñas, niños y adolescentes frente al grooming o ciberacoso. c) Capacitar a la comunidad educativa en el nivel inicial, primario y secundario de gestión pública y privada a los fines de concientizar sobre la problemática del grooming o ciberacoso. d) Diseñar y desarrollar campañas de difusión a través de los medios masivos de comunicación a los fines de cumplir con los objetivos del presente Programa. e) Brindar información acerca de cómo denunciar este tipo de delitos en la justicia. **Artículo 5º-** A los efectos de la presente ley, procúrese incluir como pantalla de inicio de teléfonos celulares, teléfonos inteligentes, tablets, y otros dispositivos tecnológicos que disponga la Autoridad de Aplicación, la siguiente información: a) Peligrosidad de sobreexposición en las redes de niñas, niños y adolescentes. b) Información acerca de la existencia de delitos cibernéticos haciendo especial énfasis en los de carácter sexual que atentan a la integridad de niñas, niños y adolescentes. c) Aconsejar el rechazo de los mensajes de tipo pornográfico. d) Advertir sobre la peligrosidad de publicar fotos propias o de amistades en sitios públicos. e) Recomendar la utilización de perfiles privados en las redes sociales. f) Sugerir no aceptar en redes sociales a personas que no hayan sido vistas físicamente y/o no sean conocidas.

		g) Respetar los derechos propios y de terceros haciendo hincapié en que todos tienen derecho a la privacidad de datos y de imágenes. h) Aconsejar el mantenimiento seguro del dispositivo electrónico y la utilización de programas para proteger el ordenador contra el software malintencionado. i) Brindar información respecto a cómo actuar ante un delito informático. j) Informar respecto a la importancia de conservar todas las pruebas tales como conversaciones, mensajes, capturas de pantalla, etc., en caso de haberse producido una situación de acoso. k) Facilitar información acerca de dónde se deben denunciar este tipo de delitos. **Artículo 6º-** Créase una página web con información referida al grooming o ciberacoso y al uso responsable de las Tecnologías de la Información y la Comunicación, destinada a la población en general y a la comunidad educativa en particular, con el fin de que obtengan material de información, prevención y capacitación. **Artículo 7º-** El Poder Ejecutivo nacional determinará la Autoridad de Aplicación de la presente ley, la cual podrá agregar contenidos si lo presume necesario. **Art. 8º-** Serán funciones de la Autoridad de Aplicación: a) Celebrar convenios con organismos estatales y no estatales que propendan a la implementación del Programa. b) Coordinar un equipo interdisciplinario integrado por profesionales especialistas en la materia, que elabore planes de acción sobre prevención y concientización. c) Organizar espacios de reflexión y debate en establecimientos educativos de gestión pública y privada y cualquier otro ámbito que reúna a niñas, niños y adolescentes y a sus padres, madres y/o tutores/as con el objeto de capacitarlos mediante talleres, seminarios y clases especiales orientadas a la concientización y conocimiento del uso responsable de las Tecnologías de la Información y la Comunicación, y de la prevención y cuidado frente al grooming o ciberacoso. d) Promover y difundir investigaciones relacionadas a la problemática del grooming o ciberacoso. e) Fiscalizar y verificar el cumplimiento de las disposiciones de la presente ley, disponiendo la aplicación de las sanciones que correspondan en caso de infracción a la misma.

	Ley 27411 Convenio sobre Ciberdelito. Aprobación.	**ARTÍCULO 1°. -** Apruébase el CONVENIO SOBRE CIBERDELITO del CONSEJO DE EUROPA[7], adoptado en la Ciudad de BUDAPEST, HUNGRÍA, el 23 de noviembre de 2001, que consta de CUARENTA Y OCHO (48) artículos cuya copia auténtica de su traducción al español, así como de su versión en idioma inglés, como ANEXO I, forma parte de la presente. **ARTÍCULO 2°. -** Al depositarse el instrumento de adhesión deberán efectuarse las siguientes reservas: a) La REPÚBLICA ARGENTINA hace reserva del artículo 6.1.b. del CONVENIO SOBRE CIBERDELITO y manifiesta que no regirá en su jurisdicción por entender que prevé un supuesto de anticipación de la pena mediante la tipificación de actos preparatorios, ajeno a su tradición legislativa en materia jurídico penal. b) La REPÚBLICA ARGENTINA hace reserva de los artículos 9.1.d., 9.2.b. y 9.2.c. del CONVENIO SOBRE CIBERDELITO y manifiesta que estos no regirán en su jurisdicción por entender que son supuestos que resultan incompatibles con el CÓDIGO PENAL vigente, conforme a la reforma introducida por la ley 26.388. c) La REPÚBLICA ARGENTINA hace reserva parcial del artículo 9.1.e. del CONVENIO SOBRE CIBERDELITO y manifiesta que no regirá en su jurisdicción por entender que el mismo sólo es aplicable de acuerdo a legislación penal vigente hasta la fecha, cuando la posesión allí referida fuera cometida con inequívocos fines de distribución o comercialización (artículo 128, segundo párrafo, del CÓDIGO PENAL). d) La REPÚBLICA ARGENTINA hace reserva del artículo 22.1.d. del CONVENIO SOBRE CIBERDELITO y manifiesta que no regirá en su jurisdicción por entender que su contenido difiere de las reglas que rigen la definición de la competencia penal nacional. e) La REPÚBLICA ARGENTINA hace reserva del artículo 29.4 del CONVENIO SOBRE CIBERDELITO y manifiesta que no regirá en su jurisdicción por entender que el requisito de la doble incriminación es una de las bases fundamentales de la LEY DE COOPERACIÓN INTERNACIONAL EN MATERIA PENAL N° 24.767 para el tipo de medidas de cooperación previstas en artículo y numeral citados.
	Decreto 577/2017 Comité de Ciberseguridad Creación.	**ARTÍCULO 1°. -** Créase el COMITÉ DE CIBERSEGURIDAD en la órbita del MINISTERIO DE MODERNIZACIÓN, que estará integrado por representantes del citado Ministerio, del MINISTERIO DE DEFENSA y del MINISTERIO DE SEGURIDAD, el cual tendrá por objetivo la elaboración de la Estrategia Nacional de Ciberseguridad. El COMITÉ DE CIBERSEGURIDAD será presidido por el MINISTRO DE MODERNIZACIÓN. **ARTÍCULO 2°. -** Son tareas del COMITÉ DE CIBERSEGURIDAD:

[7]Copia auténtica traducida al español del Convenio Sobre Ciberdelito. Ver: https://servicios.infoleg.gob.ar/infolegInternet/anexos/300000-304999/304798/ley27411.pdf

		a) Desarrollar la Estrategia Nacional de Ciberseguridad, en coordinación con las áreas competentes de la Administración Pública Nacional. b) Elaborar el plan de acción necesario para la implementación de la Estrategia Nacional de Ciberseguridad. c) Convocar a otros organismos para que participen en la implementación de medidas en el marco del plan de acción elaborado conforme lo establecido en el punto b) precedente. d) Impulsar el dictado de un marco normativo en materia de Ciberseguridad. e) Fijar los lineamientos y criterios para la definición, identificación y protección de las infraestructuras críticas nacionales. f) Participar en el desarrollo de acciones inherentes a la Ciberseguridad nacional que se le encomienden. **ARTÍCULO 3°. -** Los Ministerios integrantes del COMITÉ DE CIBERSEGURIDAD deben designar dentro del plazo de TREINTA (30) días del dictado de la presente medida, UN (1) miembro titular que deberá tener el rango de Subsecretario o Director Nacional o equivalente como mínimo, y DOS (2) miembros suplentes con rango de Director Nacional o equivalente, como mínimo. **ARTÍCULO 4°. -** El COMITÉ DE CIBERSEGURIDAD dictará su propio reglamento y fijará los lineamientos para su funcionamiento. **ARTÍCULO 5°. -** Encomiéndase al MINISTRO DE MODERNIZACIÓN, o a quien ese designe, impulsar los actos administrativos y demás acciones necesarias para la implementación de la Estrategia Nacional de Ciberseguridad que apruebe el COMITÉ DE CIBERSEGURIDAD, así como de los objetivos en ella contenidos.
Bolivia	Constitución Política del Estado	**Artículo 25.** (…). II. Son inviolables la correspondencia, los papeles privados y las manifestaciones privadas contenidas en cualquier soporte, éstos no podrán ser incautados salvo en los casos determinados por la ley para la investigación penal, en virtud de orden escrita y motivada de autoridad judicial competente. **Artículo 130.** I. Toda persona individual o colectiva que crea estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados, o que afecten a su derecho fundamental a la intimidad y privacidad personal o familiar, o a su propia imagen, honra y reputación, podrá interponer la Acción de Protección de Privacidad.

		II. La Acción de Protección de Privacidad no procederá para levantar el secreto en materia de prensa. **Artículo 131.** I. La Acción de Protección de Privacidad tendrá lugar de acuerdo con el procedimiento previsto para la acción de Amparo Constitucional. II. Si el tribunal o juez competente declara procedente la acción, ordenará la revelación, eliminación o rectificación de los datos cuyo registro fue impugnado. III. La decisión se elevará, de oficio, en revisión ante el Tribunal Constitucional Plurinacional en el plazo de las veinticuatro horas siguientes a la emisión del fallo, sin que por ello se suspenda su ejecución. IV. La decisión final que conceda la Acción de Protección de Privacidad será ejecutada inmediatamente y sin observación. En caso de resistencia se procederá de acuerdo con lo señalado en la Acción de Libertad. La autoridad judicial que no proceda conforme con lo dispuesto por este artículo quedará sujeta a las sanciones previstas por la ley.
	Código Penal	Capítulo XI DELITOS INFORMATICOS **Artículo 363 bis. - (MANIPULACIÓN INFORMÁTICA). -** El que con la intención de obtener un beneficio indebido para sí o un tercero, manipule un procesamiento o transferencia de datos informáticos que conduzca a un resultado incorrecto o evite un proceso tal cuyo resultado habría sido correcto, ocasionando de esta manera una transferencia patrimonial en perjuicio de tercero, será sancionado con reclusión de uno a cinco años y con multa de sesenta a doscientos días. **Artículo 363 ter. - (ALTERACIÓN, ACCESO Y USO INDEBIDO DE DATOS INFORMÁTICOS). -** El que sin estar autorizado se apodere, acceda, utilice, modifique, suprima o inutilice, datos almacenados en una computadora o en cualquier soporte informático, ocasionando perjuicio al titular de la información, será sancionado con prestación de trabajo hasta un año o multa hasta doscientos días.
	Ley 164 Ley de 8 de agosto de 2011 Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación	TÍTULO III TELECOMUNICACIONES CAPÍTULO ONCEAVO DERECHOS Y OBLIGACIONES DE LAS USUARIAS Y USUARIOS **Artículo 56. (INVIOLABILIDAD Y SECRETO DE LAS COMUNICACIONES).** En el marco de lo establecido en la Constitución Política del Estado, los operadores de redes públicas y proveedores de servicios de telecomunicaciones y tecnologías de información y comunicación, deben

		garantizar la inviolabilidad y secreto de las comunicaciones, al igual que la protección de los datos personales y la intimidad de usuarias o usuarios, salvo los contemplados en guías telefónicas, facturas y otros establecidos por norma. TÍTULO IV DESARROLLO DE CONTENIDOS Y APLICACIONES DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN CAPÍTULO CUARTO COMERCIO ELECTRÓNICO **Artículo 85. (LA OFERTA ELECTRÓNICA DE BIENES Y SERVICIOS).** La oferta de bienes y servicios por medios digitales, que cumplan con las condiciones generales y específicas que la Ley impone, debe ser realizada en un ambiente técnicamente confiable y en las condiciones que establece el Código de Comercio. **Artículo 86. (VALIDEZ DE LOS CONTRATOS ELECTRÓNICOS).** **I.** Las partes podrán realizar transacciones comerciales mediante documento digital en las condiciones señaladas en la Ley. **II.** Lo dispuesto en el presente capítulo no será aplicable a aquellos contratos en los cuales la Ley o el mismo contrato excluya expresamente la validez de los documentos digitales. **Artículo 87. (VALORACIÓN).** **I.** Los documentos digitales carentes de firma digital, serán admisibles como principio de prueba o indicios. **II.** Se tomará en cuenta la confiabilidad de la forma en que se haya generado, archivado y comunicado el documento digital, la forma en que se haya conservado la integridad de la información, y la forma en la que se identifique a su iniciador y cualquier otro factor pertinente. **Artículo 88. (CONTROVERSIAS).** En caso de controversias las partes se someterán a la jurisdicción estipulada en el contrato, a falta de ésta, se sujetarán a la autoridad administrativa boliviana si corresponde y en su caso a la jurisdicción ordinaria.
	Ley 548 Ley de 17 de Julio de 2014 Código Niña, Niño y Adolescente	**ARTÍCULO 151.** (TIPOS DE VIOLENCIA EN EL SISTEMA EDUCATIVO). I. A efectos del presente Código, se consideran formas de violencia en el Sistema Educativo: (…); g) **Violencia Cibernética en el Sistema Educativo**. Se presenta cuando una o un miembro de la comunidad educativa es hostigada u hostigado, amenazada o amenazado, acosada o acosado, difamada o difamado, humillada o humillado, de forma dolosa por otra u otras personas, causando angustia emocional y preocupación, a través de correos electrónicos, videojuegos conectados al internet, redes sociales, blogs, mensajería instantánea y mensajes de texto a través de internet, teléfono móvil o cualquier otra tecnología de información y comunicación.

Colombia	Constitución Política	**ARTÍCULO 15.** Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución. La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley. Para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley.
	Código Penal	Título VII BIS De la Protección de la información y de los datos CAPITULO I **De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos** **Artículo 269A.***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, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes. **Artículo 269B.***Obstaculización ilegítima de sistema informático o red de telecomunicación.* El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, 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, siempre que la conducta no constituya delito sancionado con una pena mayor. **Artículo 269C.***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. **Artículo 269D.***Daño Informático*. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o 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 1.000 salarios mínimos legales mensuales vigentes.

		Artículo 269E.*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 1.000 salarios mínimos legales mensuales vigentes. **Artículo 269F.***Violación de datos personales*. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, 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. **Artículo 269G.***Suplantación de sitios web para capturar datos personales*. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave. En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave. La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito. **Artículo 269H.***Circunstancias de agravación punitiva*: Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere: 1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros. 2. Por servidor público en ejercicio de sus funciones. 3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este. 4. Revelando o dando a conocer el contenido de la información en perjuicio de otro. 5. Obteniendo provecho para sí o para un tercero.

		6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional. 7. Utilizando como instrumento a un tercero de buena fe. 8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales. CAPITULO II **De los atentados informáticos y otras infracciones** **Artículo 269I.***Hurto por medios informáticos y semejantes*. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código. **Artículo 269J.***Transferencia no consentida de activos*. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa. Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.
	Ley 1581 De 2012 (octubre 17) Por la cual se dictan disposiciones generales para la protección de datos personales	TÍTULO I OBJETO, ÁMBITO DE APLICACIÓN Y DEFINICIONES **Artículo 1°. Objeto.** La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma. **Artículo 2°. Ámbito de aplicación.** Los principios y disposiciones contenidas en la presente ley serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada.

		La presente ley aplicará al tratamiento de datos personales efectuado en territorio colombiano o cuando al Responsable del Tratamiento o Encargado del Tratamiento no establecido en territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales. El régimen de protección de datos personales que se establece en la presente ley no será de aplicación: a) A las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico. Cuando estas bases de datos o archivos vayan a ser suministrados a terceros se deberá, de manera previa, informar al Titular y solicitar su autorización. En este caso los Responsables y Encargados de las bases de datos y archivos quedarán sujetos a las disposiciones contenidas en la presente ley; b) A las bases de datos y archivos que tengan por finalidad la seguridad y defensa nacional, así como la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo; c) A las Bases de datos que tengan como fin y contengan información de inteligencia y contrainteligencia; d) A las bases de datos y archivos de información periodística y otros contenidos editoriales; e) A las bases de datos y archivos regulados por la Ley 1266 de 2008; f) A las bases de datos y archivos regulados por la Ley 79 de 1993. **Parágrafo.** Los principios sobre protección de datos serán aplicables a todas las bases de datos, incluidas las exceptuadas en el presente artículo, con los límites dispuestos en la presente ley y sin reñir con los datos que tienen características de estar amparados por la reserva legal. En el evento que la normatividad especial que regule las bases de datos exceptuadas prevea principios que tengan en consideración la naturaleza especial de datos, los mismos aplicarán de manera concurrente a los previstos en la presente ley. (…). TÍTULO IV DERECHOS Y CONDICIONES DE LEGALIDAD PARA EL TRATAMIENTO DE DATOS **Artículo 8°.** Derechos de los Titulares. El Titular de los datos personales tendrá los siguientes derechos:

		a) Conocer, actualizar y rectificar sus datos personales frente a los Responsables del Tratamiento o Encargados del Tratamiento. Este derecho se podrá ejercer, entre otros frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo Tratamiento esté expresamente prohibido o no haya sido autorizado; b) Solicitar prueba de la autorización otorgada al Responsable del Tratamiento salvo cuando expresamente se exceptúe como requisito para el Tratamiento, de conformidad con lo previsto en el artículo 10 de la presente ley; c) Ser informado por el Responsable del Tratamiento o el Encargado del Tratamiento, previa solicitud, respecto del uso que le ha dado a sus datos personales; d) Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la presente ley y las demás normas que la modifiquen, adicionen o complementen; e) Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el Tratamiento el Responsable o Encargado han incurrido en conductas contrarias a esta ley y a la Constitución; f) Acceder en forma gratuita a sus datos personales que hayan sido objeto de Tratamiento. **Artículo 9°.** Autorización del Titular. Sin perjuicio de las excepciones previstas en la ley, en el Tratamiento se requiere la autorización previa e informada del Titular, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta posterior. **Artículo 10.** Casos en que no es necesaria la autorización. La autorización del Titular no será necesaria cuando se trate de: a) Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial; b) Datos de naturaleza pública; c) Casos de urgencia médica o sanitaria; d) Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos; e) Datos relacionados con el Registro Civil de las Personas. Quien acceda a los datos personales sin que medie autorización previa deberá en todo caso cumplir con las disposiciones contenidas en la presente ley.

		Artículo 11. Suministro de la información. La información solicitada podrá ser suministrada por cualquier medio, incluyendo los electrónicos, según lo requiera el Titular. La información deberá ser de fácil lectura, sin barreras técnicas que impidan su acceso y deberá corresponder en un todo a aquella que repose en la base de datos. El Gobierno Nacional establecerá la forma en la cual los Responsables del Tratamiento y Encargados del Tratamiento deberán suministrar la información del Titular, atendiendo a la naturaleza del dato personal, Esta reglamentación deberá darse a más tardar dentro del año siguiente a la promulgación de la presente ley. **Artículo 12.** Deber de informar al Titular. El Responsable del Tratamiento, al momento de solicitar al Titular la autorización, deberá informarle de manera clara y expresa lo siguiente: a) El Tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo; b) El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando estas versen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes; c) Los derechos que le asisten como Titular; d) La identificación, dirección física o electrónica y teléfono del Responsable del Tratamiento. **Parágrafo.** El Responsable del Tratamiento deberá conservar prueba del cumplimiento de lo previsto en el presente artículo y, cuando el Titular lo solicite, entregarle copia de esta. **Artículo 13.** Personas a quienes se les puede suministrar la información. La información que reúna las condiciones establecidas en la presente ley podrá suministrarse a las siguientes personas: a) A los Titulares, sus causahabientes o sus representantes legales; b) A las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial; c) A los terceros autorizados por el Titular o por la ley. (…). TÍTULO VI DEBERES DE LOS RESPONSABLES DEL TRATAMIENTO Y ENCARGADOS DEL TRATAMIENTO

		Artículo 17. Deberes de los Responsables del Tratamiento. Los Responsables del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad: a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data; b) Solicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el Titular; c) Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada; d) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento; e) Garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible; f) Actualizar la información, comunicando de forma oportuna al Encargado del Tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada; g) Rectificar la información cuando sea incorrecta y comunicar lo pertinente al Encargado del Tratamiento; h) Suministrar al Encargado del Tratamiento, según el caso, únicamente datos cuyo Tratamiento esté previamente autorizado de conformidad con lo previsto en la presente ley; i) Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular; j) Tramitar las consultas y reclamos formulados en los términos señalados en la presente ley; k) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y en especial, para la atención de consultas y reclamos; l) Informar al Encargado del Tratamiento cuando determinada información se encuentra en discusión por parte del Titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo; m) Informar a solicitud del Titular sobre el uso dado a sus datos;

		n) Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares. o) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio. **Artículo 18.** Deberes de los Encargados del Tratamiento. Los Encargados del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad: a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data; b) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento; c) Realizar oportunamente la actualización, rectificación o supresión de los datos en los términos de la presente ley; d) Actualizar la información reportada por los Responsables del Tratamiento dentro de los cinco (5) días hábiles contados a partir de su recibo; e) Tramitar las consultas y los reclamos formulados por los Titulares en los términos señalados en la presente ley; f) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y, en especial, para la atención de consultas y reclamos por parte de los Titulares; g) Registrar en la base de datos las leyenda "reclamo en trámite" en la forma en que se regula en la presente ley; h) Insertar en la base de datos la leyenda "información en discusión judicial" una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal; i) Abstenerse de circular información que esté siendo controvertida por el Titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio; j) Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella; k) Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares; l) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

		Parágrafo. En el evento en que concurran las calidades de Responsable del Tratamiento y Encargado del Tratamiento en la misma persona, le será exigible el cumplimiento de los deberes previstos para cada uno. TÍTULO VII DE LOS MECANISMOS DE VIGILANCIA Y SANCIÓN CAPÍTULO I **De la autoridad de protección de datos** **Artículo 19.** Autoridad de Protección de Datos. La Superintendencia de Industria y Comercio, a través de una Delegatura para la Protección de Datos Personales, ejercerá la vigilancia para garantizar que en el Tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la presente ley. **Parágrafo 1°.** El Gobierno Nacional en el plazo de seis (6) meses contados a partir de la fecha de entrada en vigencia de la presente ley incorporará dentro de la estructura de la Superintendencia de Industria y Comercio un despacho de Superintendente Delegado para ejercer las funciones de Autoridad de Protección de Datos. **Parágrafo 2°.** La vigilancia del tratamiento de los datos personales regulados en la Ley 1266 de 2008 se sujetará a lo previsto en dicha norma. **Artículo 20.** Recursos para el ejercicio de sus funciones. La Superintendencia de Industria y Comercio contará con los siguientes recursos para ejercer las funciones que le son atribuidas por la presente ley: a) Los recursos que le sean destinados en el Presupuesto General de la Nación. **Artículo 21.** Funciones. La Superintendencia de Industria y Comercio ejercerá las siguientes funciones: a) Velar por el cumplimiento de la legislación en materia de protección de datos personales; b) Adelantar las investigaciones del caso, de oficio o a petición de parte y, como resultado de ellas, ordenar las medidas que sean necesarias para hacer efectivo el derecho de hábeas data. Para el efecto, siempre que se desconozca el derecho, podrá disponer que se conceda el acceso y suministro de los datos, la rectificación, actualización o supresión de los mismos; c) Disponer el bloqueo temporal de los datos cuando, de la solicitud y de las pruebas aportadas por el Titular, se identifique un riesgo cierto de vulneración de sus derechos fundamentales, y dicho bloqueo sea necesario para protegerlos mientras se adopta una decisión definitiva;

		d) Promover y divulgar los derechos de las personas en relación con el Tratamiento de datos personales e implementará campañas pedagógicas para capacitar e informar a los ciudadanos acerca del ejercicio y garantía del derecho fundamental a la protección de datos; e) Impartir instrucciones sobre las medidas y procedimientos necesarios para la adecuación de las operaciones de los Responsables del Tratamiento y Encargados del Tratamiento a las disposiciones previstas en la presente ley; f) Solicitar a los Responsables del Tratamiento y Encargados del Tratamiento la información que sea necesaria para el ejercicio efectivo de sus funciones. g) Proferir las declaraciones de conformidad sobre las transferencias internacionales de datos; h) Administrar el Registro Nacional Público de Bases de Datos y emitir las órdenes y los actos necesarios para su administración y funcionamiento; i) Sugerir o recomendar los ajustes, correctivos o adecuaciones a la normatividad que resulten acordes con la evolución tecnológica, informática o comunicacional; j) Requerir la colaboración de entidades internacionales o extranjeras cuando se afecten los derechos de los Titulares fuera del territorio colombiano con ocasión, entre otras, de la recolección internacional de datos personajes; k) Las demás que le sean asignadas por ley. (…). CAPÍTULO III Del Registro Nacional de Bases de Datos **Artículo 25.** Definición. El Registro Nacional de Bases de Datos es el directorio público de las bases de datos sujetas a Tratamiento que operan en el país. El registro será administrado por la Superintendencia de Industria y Comercio y será de libre consulta para los ciudadanos. Para realizar el registro de bases de datos, los interesados deberán aportar a la Superintendencia de Industria y Comercio las políticas de tratamiento de la información, las cuales obligarán a los responsables y encargados del mismo, y cuyo incumplimiento acarreará las sanciones correspondientes. Las políticas de Tratamiento en ningún caso podrán ser inferiores a los deberes contenidos en la presente ley. **Parágrafo.** El Gobierno Nacional reglamentará, dentro del año siguiente a la promulgación de la presente ley, la información mínima que debe contener el Registro, y los términos y condiciones bajo los cuales se deben inscribir en este los Responsables del Tratamiento.

		TÍTULO VIII TRANSFERENCIA DE DATOS A TERCEROS PAÍSES **Artículo 26.** Prohibición. Se prohíbe la transferencia de datos personales de cualquier tipo a países que no proporcionen niveles adecuados de protección de datos. Se entiende que un país ofrece un nivel adecuado de protección de datos cuando cumpla con los estándares fijados por la Superintendencia de Industria y Comercio sobre la materia, los cuales en ningún caso podrán ser inferiores a los que la presente ley exige a sus destinatarios. Esta prohibición no regirá cuando se trate de: a) Información respecto de la cual el Titular haya otorgado su autorización expresa e inequívoca para la transferencia; b) Intercambio de datos de carácter médico, cuando así lo exija el Tratamiento del Titular por razones de salud o higiene pública; c) Transferencias bancarias o bursátiles, conforme a la legislación que les resulte aplicable; d) Transferencias acordadas en el marco de tratados internacionales en los cuales la República de Colombia sea parte, con fundamento en el principio de reciprocidad; e) Transferencias necesarias para la ejecución de un contrato entre el Titular y el Responsable del Tratamiento, o para la ejecución de medidas precontractuales siempre y cuando se cuente con la autorización del Titular; f) Transferencias legalmente exigidas para la salvaguardia del interés público, o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial. **Parágrafo 1°.** En los casos no contemplados como excepción en el presente artículo, corresponderá a la Superintendencia de Industria y Comercio, proferir la declaración de conformidad relativa a la transferencia internacional de datos personales. Para el efecto, el Superintendente queda facultado para requerir información y adelantar las diligencias tendientes a establecer el cumplimiento de los presupuestos que requiere la viabilidad de la operación. **Parágrafo 2°.** Las disposiciones contenidas en el presente artículo serán aplicables para todos los datos personales, incluyendo aquellos contemplados en la Ley 1266 de 2008.
	Ley 1266 de 2008 (diciembre 31)	**ARTÍCULO 1o. OBJETO.** La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos, y los demás derechos, libertades y garantías constitucionales

	Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.	relacionadas con la recolección, tratamiento y circulación de datos personales a que se refiere el artículo 15 de la Constitución Política, así como el derecho a la información establecido en el artículo 20 de la Constitución Política, particularmente en relación con la información financiera y crediticia, comercial, de servicios y la proveniente de terceros países. **ARTÍCULO 2o. AMBITO DE APLICACIÓN**. La presente ley se aplica a todos los datos de información personal registrados en un banco de datos, sean estos administrados por entidades de naturaleza pública o privada. Esta ley se aplicará sin perjuicio de normas especiales que disponen la confidencialidad o reserva de ciertos datos o información registrada en bancos de datos de naturaleza pública, para fines estadísticos, de investigación o sanción de delitos o para garantizar el orden público. Se exceptúan de esta ley las bases de datos que tienen por finalidad producir la Inteligencia de Estado por parte del Departamento Administrativo de Seguridad, DAS, y de la Fuerza Pública para garantizar la seguridad nacional interna y externa. Los registros públicos a cargo de las cámaras de comercio se regirán exclusivamente por las normas y principios consagrados en las normas especiales que las regulan. Igualmente, quedan excluidos de la aplicación de la presente ley aquellos datos mantenidos en un ámbito exclusivamente personal o doméstico y aquellos que circulan internamente, esto es, que no se suministran a otras personas jurídicas o naturales. (…). TITULO II. DERECHOS DE LOS TITULARES DE LA INFORMACION. **ARTÍCULO 6o. DERECHOS DE LOS TITULARES DE LA INFORMACIÓN**. Los titulares tendrán los siguientes derechos: 1. Frente a los operadores de los bancos de datos: 1.1 Ejercer el derecho fundamental al hábeas data en los términos de la presente ley, mediante la utilización de los procedimientos de consultas o reclamos, sin perjuicio de los demás mecanismos constitucionales y legales. 1.2 Solicitar el respeto y la protección de los demás derechos constitucionales o legales, así como de las demás disposiciones de la presente ley, mediante la utilización del procedimiento de reclamos y peticiones. 1.3 Solicitar prueba de la certificación de la existencia de la autorización expedida por la fuente o por el usuario. 1.4 Solicitar información acerca de los usuarios autorizados para obtener información. PARÁGRAFO. La administración de información pública no requiere autorización del titular de los datos, pero se sujeta al cumplimiento de los principios de la administración de datos personales y a las demás disposiciones de la presente ley.

		La administración de datos semiprivados y privados requiere el consentimiento previo y expreso del titular de los datos, salvo en el caso del dato financiero, crediticio, comercial, de servicios y el proveniente de terceros países el cual no requiere autorización del titular. En todo caso, la administración de datos semiprivados y privados se sujeta al cumplimiento de los principios de la administración de datos personales y a las demás disposiciones de la presente ley. 2. Frente a las fuentes de la información: 2.1 <Numeral CONDICIONALMENTE exequible> Ejercer los derechos fundamentales al hábeas data y de petición, cuyo cumplimiento se podrá realizar a través de los operadores, conforme lo previsto en los procedimientos de consultas y reclamos de esta ley, sin perjuicio de los demás mecanismos constitucionales o legales. 2.2 Solicitar información o pedir la actualización o rectificación de los datos contenidos en la base de datos, lo cual realizará el operador, con base en la información aportada por la fuente, conforme se establece en el procedimiento para consultas, reclamos y peticiones. 2.3 Solicitar prueba de la autorización, cuando dicha autorización sea requerida conforme lo previsto en la presente ley. 3. Frente a los usuarios: 3.1 Solicitar información sobre la utilización que el usuario le está dando a la información, cuando dicha información no hubiere sido suministrada por el operador. 3.2 Solicitar prueba de la autorización, cuando ella sea requerida conforme lo previsto en la presente ley. PARÁGRAFO. Los titulares de información financiera y crediticia tendrán adicionalmente los siguientes derechos: Podrán acudir ante la autoridad de vigilancia para presentar quejas contra las fuentes, operadores o usuarios por violación de las normas sobre administración de la información financiera y crediticia. Así mismo, pueden acudir ante la autoridad de vigilancia para pretender que se ordene a un operador o fuente la corrección o actualización de sus datos personales, cuando ello sea procedente conforme lo establecido en la presente ley. TITULO III. DEBERES DE LOS OPERADORES, LAS FUENTES Y LOS USUARIOS DE INFORMACION. **ARTÍCULO 7o. DEBERES DE LOS OPERADORES DE LOS BANCOS DE DATOS.** Sin perjuicio del cumplimiento de las demás disposiciones contenidas en la presente ley y otras que rijan su actividad, los operadores de los bancos de datos están obligados a:

		1. Garantizar, en todo tiempo al titular de la información, el pleno y efectivo ejercicio del derecho de hábeas data y de petición, es decir, la posibilidad de conocer la información que sobre él exista o repose en el banco de datos, y solicitar la actualización o corrección de datos, todo lo cual se realizará por conducto de los mecanismos de consultas o reclamos, conforme lo previsto en la presente ley. 2. Garantizar, que en la recolección, tratamiento y circulación de datos, se respetarán los demás derechos consagrados en la ley. 3. Permitir el acceso a la información únicamente a las personas que, de conformidad con lo previsto en esta ley, pueden tener acceso a ella. 4. Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y, en especial, para la atención de consultas y reclamos por parte de los titulares. 5. Solicitar la certificación a la fuente de la existencia de la autorización otorgada por el titular, cuando dicha autorización sea necesaria, conforme lo previsto en la presente ley. 6. Conservar con las debidas seguridades los registros almacenados para impedir su deterioro, pérdida, alteración, uso no autorizado o fraudulento. 7. Realizar periódica y oportunamente la actualización y rectificación de los datos, cada vez que le reporten novedades las fuentes, en los términos de la presente ley. 8. Tramitar las peticiones, consultas y los reclamos formulados por los titulares de la información, en los términos señalados en la presente ley. 9. Indicar en el respectivo registro individual que determinada información se encuentra en discusión por parte de su titular, cuando se haya presentado la solicitud de rectificación o actualización de la misma y no haya finalizado dicho trámite, en la forma en que se regula en la presente ley. 10. Circular la información a los usuarios dentro de los parámetros de la presente ley. 11. Cumplir las instrucciones y requerimientos que la autoridad de vigilancia imparta en relación con el cumplimiento de la presente ley. 12. Los demás que se deriven de la Constitución o de la presente ley. **ARTÍCULO 8o. DEBERES DE LAS FUENTES DE LA INFORMACIÓN.** Las fuentes de la información deberán cumplir las siguientes obligaciones, sin perjuicio del cumplimiento de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:

		1. Garantizar que la información que se suministre a los operadores de los bancos de datos o a los usuarios sea veraz, completa, exacta, actualizada y comprobable. 2. Reportar, de forma periódica y oportuna al operador, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada. 3. Rectificar la información cuando sea incorrecta e informar lo pertinente a los operadores. 4. Diseñar e implementar mecanismos eficaces para reportar oportunamente la información al operador. 5. Solicitar, cuando sea del caso, y conservar copia o evidencia de la respectiva autorización otorgada por los titulares de la información, y asegurarse de no suministrar a los operadores ningún dato cuyo suministro no esté previamente autorizado, cuando dicha autorización sea necesaria, de conformidad con lo previsto en la presente ley. 6. Certificar, semestralmente al operador, que la información suministrada cuenta con la autorización de conformidad con lo previsto en la presente ley. 7. Resolver los reclamos y peticiones del titular en la forma en que se regula en la presente ley. 8. Informar al operador que determinada información se encuentra en discusión por parte de su titular, cuando se haya presentado la solicitud de rectificación o actualización de la misma, con el fin de que el operador incluya en el banco de datos una mención en ese sentido hasta que se haya finalizado dicho trámite. 9. Cumplir con las instrucciones que imparta la autoridad de control en relación con el cumplimiento de la presente ley. 10. Los demás que se deriven de la Constitución o de la presente ley. 11. Reportar la información negativa de los titulares, máximo (18) meses después de la constitución en mora del titular. **ARTÍCULO 9o. DEBERES DE LOS USUARIOS**. Sin perjuicio del cumplimiento de las disposiciones contenidas en la presente ley y demás que rijan su actividad, los usuarios de la información deberán: 1. Guardar sobre la información que les sea suministrada por los operadores de los bancos de datos, por las fuentes o los titulares de la información y utilizar la información únicamente para los fines para los que le fue entregada, en los términos de la presente ley.

		2. Informar a los titulares, a su solicitud, sobre la utilización que le está dando a la información. 3. Conservar con las debidas seguridades la información recibida para impedir su deterioro, pérdida, alteración, uso no autorizado o fraudulento. 4. Cumplir con las instrucciones que imparta la autoridad de control, en relación con el cumplimiento de la presente ley. 5. Los demás que se deriven de la Constitución o de la presente ley. TITULO IV. DE LOS BANCOS DE DATOS DE INFORMACION FINANCIERA, CREDITICIA, COMERCIAL, DE SERVICIOS Y LA PROVENIENTE DE TERCEROS PAISES. **ARTÍCULO 10. PRINCIPIO DE FAVORECIMIENTO A UNA ACTIVIDAD DE INTERÉS PÚBLICO.** La actividad de administración de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países está directamente relacionada y favorece una actividad de interés público, como lo es la actividad financiera propiamente, por cuanto ayuda a la democratización del crédito, promueve el desarrollo de la actividad de crédito, la protección de la confianza pública en el sistema financiero y la estabilidad del mismo, y genera otros beneficios para la economía nacional y en especial para la actividad financiera, crediticia, comercial y de servicios del país. PARÁGRAFO 1o. La administración de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, por parte de fuentes, usuarios y operadores deberá realizarse de forma que permita favorecer los fines de expansión y democratización del crédito. Los usuarios de este tipo de información deberán valorar este tipo de información en forma concurrente con otros factores o elementos de juicio que técnicamente inciden en el estudio de riesgo y el análisis crediticio, y no podrán basarse exclusivamente en la información relativa al incumplimiento de obligaciones suministrada por los operadores para adoptar decisiones frente a solicitudes de crédito. La Superintendencia Financiera de Colombia podrá imponer las sanciones previstas en la presente ley a los usuarios de la información que nieguen una solicitud de crédito basados exclusivamente en el reporte de información negativa del solicitante, para lo cual la institución o entidad que conforma el sistema financiero y asegurador en caso de rechazo de la solicitud del crédito, por solicitud del titular, le indicará por escrito las razones objetivas del rechazo del mismo. PARÁGRAFO 2o. La consulta de la información financiera, crediticia, comercial, de servicios y la proveniente de terceros países por parte del titular, en toda ocasión y por todos los medios, será gratuita. La revisión continua de esta información por parte del titular o usuario no podrá ser causal de disminución en la calificación de riesgo, récord (scorfngs-score), o cualquier tipo de medición, ni podrá alterar en nada los estudios financieros o crediticios. En ningún caso se podrá consultar esta información para fines de toma de decisiones laborales, y no podrá utilizarse para fines diferentes al análisis o cálculo del riesgo crediticio del titular del dato.

		ARTÍCULO 11. REQUISITOS ESPECIALES PARA LOS OPERADORES. Los operadores de bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países que funcionen como entes independientes a las fuentes de la información, deberán cumplir con los siguientes requisitos especiales de funcionamiento: 1. Deberán constituirse como sociedades comerciales, entidades sin ánimo de lucro, o entidades cooperativas. 2. Deberán contar con un área de servicio al titular de la información, para la atención de peticiones, consultas y reclamos. 3. Deberán contar con un sistema de seguridad y con las demás condiciones técnicas suficientes para garantizar la seguridad y actualización de los registros, evitando su adulteración, pérdida, consulta o uso no autorizado conforme lo previsto en la presente ley. 4. Deberán actualizar la información reportada por las fuentes con una periodicidad no superior a diez (10) días calendario contados a partir del recibo de la misma. **ARTÍCULO 12. REQUISITOS ESPECIALES PARA FUENTES.** Las fuentes deberán actualizar mensualmente la información suministrada al operador, sin perjuicio de lo dispuesto en el Título III de la presente ley. El reporte de información negativa sobre incumplimiento de obligaciones de cualquier naturaleza, que hagan las fuentes de información a los operadores de bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, sólo procederá previa comunicación al titular de la información, con el fin de que este pueda demostrar o efectuar el pago de la obligación, así como controvertir aspectos tales como el monto de la obligación o cuota y la fecha de exigibilidad. Dicha comunicación podrá incluirse en los extractos periódicos que las fuentes de información envíen a sus clientes. En todo caso, las fuentes de información podrán efectuar el reporte de la información transcurridos veinte (20) días calendario siguientes a la fecha de envío de la comunicación en la última dirección de domicilio del afectado que se encuentre registrada en los archivos de la fuente de la información y sin perjuicio, si es del caso, de dar cumplimiento a la obligación de informar al operador, que la información se encuentra en discusión por parte de su titular, cuando se haya presentado solicitud de rectificación o actualización y esta aún no haya sido resuelta. PARÁGRAFO. El incumplimiento de la comunicación previa al titular de la información, en los casos en que la obligación o cuota ya haya sido extinguida, dará lugar al retiro inmediato del reporte negativo. En los casos en que se genere el reporte sin el cumplimiento de la comunicación y no se haya extinguido la obligación o cuota, se deberá retirar el reporte y cumplir con la comunicación antes de realizarlo nuevamente. **ARTÍCULO 13. PERMANENCIA DE LA INFORMACIÓN**. La información de carácter positivo permanecerá de manera indefinida en los bancos de datos de los operadores de información. Los datos cuyo contenido haga referencia al tiempo de mora, tipo de cobro, estado de la cartera y, en general, aquellos datos referentes a una situación de incumplimiento de obligaciones, se regirán por un término máximo de permanencia, vencido

		el cual deberá ser retirada de los bancos de datos por el operador, de forma que los usuarios no puedan acceder o consultar dicha información. El término de permanencia de ésta información será el doble del tiempo de la mora, máximo cuatro (4) años contados a partir de la fecha en que sean pagadas las cuotas vencidas o sea extinguida la obligación. PARÁGRAFO 1o. El dato negativo y los datos cuyo contenido haga referencia al tiempo de mora, tipo de cobro, estado de la cartera y, en general, aquellos datos referentes a una situación de incumplimiento de obligaciones caducarán una vez cumplido el término de ocho (8) años, contados a partir del momento en que entre en mora la obligación; cumplido este término deberán ser eliminados de la base de datos. PARÁGRAFO 2o. En las obligaciones inferiores o iguales al (15%) de un (1) salario mínimo legal mensual vigente, el dato negativo por obligaciones que se han constituido en mora solo será reportado después de cumplirse con al menos dos comunicaciones, ambas en días diferentes. Y debe mediar entre la última comunicación y reporte, 20 días calendario. PARÁGRAFO 3o. Toda información negativa o desfavorable que se encuentre en bases de datos y se relacione con calificaciones, récord (scorings-score), o cualquier tipo de medición financiera, comercial o crediticia, deberá ser actualizada de manera simultánea con el retiro del dato negativo o con la cesación del hecho que generó la disminución de la medición. **ARTÍCULO 14. CONTENIDO DE LA INFORMACIÓN**. El Gobierno Nacional establecerá la forma en la cual los bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, deberán presentar la información de los titulares de la información. Para tal efecto, deberá señalar un formato que permita identificar, entre otros aspectos, el nombre completo del deudor, la condición en que actúa, esto es, como deudor principal, deudor solidario, avalista o fiador, el monto de la obligación o cuota vencida, el tiempo de mora y la fecha del pago, si es del caso. El Gobierno Nacional al ejercer la facultad prevista en el inciso anterior deberá tener en cuenta que en el formato de reporte deberá establecer que: a) <Literal CONDICIONALMENTE exequible> Se presenta reporte negativo cuando la(s) persona(s) naturales o jurídicas efectivamente se encuentran en mora en sus cuotas u obligaciones. b) <Literal CONDICIONALMENTE exequible> Se presenta reporte positivo cuando la(s) persona(s) naturales y jurídicas están al día en sus obligaciones. El incumplimiento de la obligación aquí prevista dará lugar a la imposición de las máximas sanciones previstas en la presente ley. PARÁGRAFO 1o. Para los efectos de la presente ley se entiende que una obligación ha sido voluntariamente pagada, cuando su pago se ha producido sin que medie sentencia judicial que así lo ordene.

		PARÁGRAFO 2o. Las consecuencias previstas en el presente artículo para el pago voluntario de las obligaciones vencidas, será predicable para cualquier otro modo de extinción de las obligaciones, que no sea resultado de una sentencia judicial. PARÁGRAFO 3o. Cuando un usuario consulte el estado de un titular en las bases de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, estas tendrán que dar información exacta sobre su estado actual, es decir, dar un reporte positivo de los usuarios que en el momento de la consulta están al día en sus obligaciones y uno negativo de los que al momento de la consulta se encuentren en mora en una cuota u obligaciones. El resto de la información contenida en las bases de datos financieros, crediticios, comercial, de servicios y la proveniente de terceros países hará parte del historial crediticio de cada usuario, el cual podrá ser consultado por el usuario, siempre y cuando hubiere sido informado sobre el estado actual. PARÁGRAFO 4o. Se prohíbe la administración de datos personales con información exclusivamente desfavorable. **ARTÍCULO 15. ACCESO A LA INFORMACIÓN POR PARTE DE LOS USUARIOS.** La información contenida en bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países podrá ser accedida por los usuarios únicamente con las siguientes finalidades: Como elemento de análisis para establecer y mantener una relación contractual, cualquiera que sea su naturaleza, así como para la evaluación de los riesgos derivados de una relación contractual vigente. Como elemento de análisis para hacer estudios de mercado o investigaciones comerciales o estadísticas. Para el adelantamiento de cualquier trámite ante una autoridad pública o una persona privada, respecto del cual dicha información resulte pertinente. Para cualquier otra finalidad, diferente de las anteriores, respecto de la cual y en forma general o para cada caso particular se haya obtenido autorización por parte del titular de la información. (…).
Costa Rica	Constitución Política	**ARTÍCULO 24.-** Se garantiza el derecho a la intimidad, a la libertad y al secreto de las comunicaciones. Son inviolables los documentos privados y las comunicaciones escritas, orales o de cualquier otro tipo de los habitantes de la República. Sin embargo, la ley, cuya aprobación y reforma requerirá los votos de dos tercios de los Diputados de la Asamblea Legislativa, fijará en qué casos podrán los Tribunales de Justicia ordenar el secuestro, registro o examen de los documentos privados, cuando sea absolutamente indispensable para esclarecer asuntos sometidos a su conocimiento.

		Toda persona tiene el derecho fundamental al acceso a las telecomunicaciones, y tecnologías de la información y comunicaciones en todo el territorio nacional. El Estado garantizará, protegerá y preservará este derecho. Igualmente, la ley determinará en cuáles casos podrán los Tribunales de Justicia ordenar que se intervenga cualquier tipo de comunicación e indicará los delitos en cuya investigación podrá autorizarse el uso de esta potestad excepcional y durante cuánto tiempo. Asimismo, señalará las responsabilidades y sanciones en que incurrirán los funcionarios que apliquen ilegalmente esta excepción. Las resoluciones judiciales amparadas a esta norma deberán ser razonadas y podrán ejecutarse de inmediato. Su aplicación y control serán responsabilidad indelegable de la autoridad judicial. La ley fijará los casos en que los funcionarios competentes del Ministerio de Hacienda y de la Contraloría General de la República podrán revisar los libros de contabilidad y sus anexos para fines tributarios y para fiscalizar la correcta utilización de los fondos públicos. Una ley especial, aprobada por dos tercios del total de los Diputados, determinará cuáles otros órganos de la Administración Pública podrán revisar los documentos que esa ley señale en relación con el cumplimiento de sus competencias de regulación y vigilancia para conseguir fines públicos. Asimismo, indicará en qué casos procede esa revisión. No producirán efectos legales, la correspondencia que fuere sustraída ni la información obtenida como resultado de la intervención ilegal de cualquier comunicación.
	Código Penal	**Artículo 167- Corrupción.** Será sancionado con pena de prisión de cuatro a nueve años, quien mantenga o promueva la corrupción de una persona menor de edad o incapaz, con fines eróticos, pornográficos u obscenos, en exhibiciones o espectáculos públicos o privados, aunque la persona menor de edad o incapaz lo consienta. La pena será de seis a doce años de prisión, si el actor, utilizando las redes sociales o cualquier otro medio informático o telemático, u otro medio de comunicación, busca encuentros de carácter sexual para sí, para otro o para grupos, con una persona menor de edad o incapaz; utiliza a estas personas para promover la corrupción o las obliga o instiga a realizar actos sexuales, prematuros, aunque la victima consienta participar en ellos o verlos ejecutar. **Artículo 167 bis- Seducción o encuentros con persona menor de edad o incapaz por medios electrónicos**. Será reprimido con prisión de dos a cuatro años quien, por cualquier medio, establezca comunicaciones de contenido sexual o erótico, ya sea que incluyan o no imágenes, videos, textos o audios, con una persona menor de edad o incapaz. La misma pena se impondrá a quien suplantando la identidad de un tercero o mediante el uso de una identidad falsa, por cualquier medio, procure establecer comunicaciones de contenido sexual o erótico, ya sea que se incluyan o no imágenes, videos, textos o audios, con una persona menor de edad o incapaz.

		La pena será de tres a cinco años, en las conductas descritas en los dos párrafos anteriores, cuando el actor procure un encuentro personal en algún lugar físico con una persona menor de edad o incapaz. (…). **Artículo 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, modifique, altere, suprima, intervenga, intercepte, abra, entregue, venda, remita o desvíe de su destino documentación o comunicaciones dirigidas a otra persona. La misma sanción indicada en el párrafo anterior se impondrá a quien, con peligro o daño para la intimidad de otro, utilice o difunda el contenido de comunicaciones o documentos privados que carezcan de interés público. 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 articulo 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, modifique, interfiera, acceda, copie, transmita, publique, difunda, recopile, inutilice, intercepte, retenga, venda, compre, 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 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.

		No constituye delito la publicación, difusión o transmisión de información de interés público, documentos públicos, datos contenidos en registros públicos o bases de datos públicos de acceso irrestricto cuando se haya tenido acceso de conformidad con los procedimientos y limitaciones de ley. Tampoco constituye delito la recopilación, copia y uso por parte de las entidades financieras supervisadas por la Sugef de la información y datos contenidos en bases de datos de origen legítimo de conformidad con los procedimientos y limitaciones de ley. (…). **Artículo 214.- Extorsión** Será reprimido con pena de prisión de cuatro a ocho años al que para procurar un lucro obligue a otro, con intimidación o con amenazas graves, a tomar una disposición patrimonial perjudicial para sí mismo o para un tercero. La pena será de cinco a diez años de prisión cuando la conducta se realice valiéndose de cualquier manipulación informática, telemática, electrónica o tecnológica. (…). **Artículo 217 bis. - Estafa informática** Se impondrá prisión de tres a seis años a quien, en perjuicio de una persona física o jurídica, manipule o influya en el ingreso, en el procesamiento o en el resultado de los datos de un sistema automatizado de información, ya sea mediante el uso de datos falsos o incompletos, el uso indebido de datos, programación, valiéndose de alguna operación informática o artificio tecnológico, o bien, por cualquier otra acción que incida en el procesamiento de los datos del sistema o que dé como resultado información falsa, incompleta o fraudulenta, con la cual procure u obtenga un beneficio patrimonial o indebido para sí o para otro. La pena será de cinco a diez años de prisión, si las conductas son cometidas contra sistemas de información públicos, sistemas de información bancarios y de entidades financieras, o cuando el autor es 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. (…). **Artículo 229.- Daño agravado** Se impondrá prisión de seis meses a cuatro años: (…). **6)** Cuando el daño recayera sobre redes, sistemas o equipos informáticos, telemáticos o electrónicos, o sus componentes físicos, lógicos o periféricos.

		Artículo 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. **Artículo 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. Sección VIII Delitos informáticos y conexos **Artículo 230.- Suplantación de identidad.** Será sancionado con pena de prisión de uno a tres años quien suplante la identidad de una persona física, jurídica o de una marca comercial en cualquiera red social, sitio de Internet, medio electrónico o tecnológico de información. **Artículo 231.- Espionaje informático** Se impondrá prisión de tres a seis años al que, sin autorización del titular o responsable, valiéndose de cualquier manipulación informática o tecnológica, se apodere, transmita, copie, modifique, destruya, utilice, bloquee o recicle información de valor para el tráfico económico de la industria y el comercio. **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. **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. **Artículo 233.- Suplantación de páginas electrónicas** Se impondrá pena de prisión de uno a tres años a quien, en perjuicio de un tercero, suplante sitios legítimos de la red de Internet.

		La pena será de tres a seis años de prisión cuando, como consecuencia de la suplantación del sitio legítimo de Internet y mediante engaño o haciendo incurrir en error, capture información confidencial de una persona física o jurídica para beneficio propio o de un tercero. **Artículo 234.- Facilitación del delito informático** Se impondrá pena de prisión de uno a cuatro años a quien facilite los medios para la consecución de un delito efectuado mediante un sistema o red informática o telemática, o los contenedores electrónicos, ópticos o magnéticos. **Artículo 235.- Narcotráfico y crimen organizado** La pena se duplicará cuando cualquiera de los delitos cometidos por medio de un sistema o red informática o telemática, o los contenedores electrónicos, ópticos o magnéticos afecte la lucha contra el narcotráfico o el crimen organizado. **Artículo 236.- Difusión de información falsa** Será sancionado con pena de tres a seis años de prisión quien, a través de medios electrónicos, informáticos, o mediante un sistema de telecomunicaciones, propague o difunda noticias o hechos falsos capaces de distorsionar o causar perjuicio a la seguridad y estabilidad del sistema financiero o de sus usuarios.
Chile	Constitución Política de la República	**Artículo 19.-** La Constitución asegura a todas las personas: 1°.- El derecho a la vida y a la integridad física y psíquica de la persona. (…). El desarrollo científico y tecnológico estará al servicio de las personas y se llevará a cabo con respeto a la vida y a la integridad física y psíquica. La ley regulará los requisitos, condiciones y restricciones para su utilización en las personas, debiendo resguardar especialmente la actividad cerebral, así como la información proveniente de ella; (…); 4°.- El respeto y protección a la vida privada y a la honra de la persona y su familia, y asimismo, la protección de sus datos personales. El tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley; (…).
	Ley 21459 Establece normas sobre delitos informáticos, deroga la Ley 19.223 y modifica otros cuerpos legales con el objeto de	**Artículo 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.

	adecuarlos al Convenio de Budapest	**Artículo 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. **Artículo 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. **Artículo 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. **Artículo 5°. -** Falsificación informática. El que indebidamente introduzca, altere, dañe o suprima datos informáticos con la intención de que sean tomados como auténticos o utilizados para generar documentos auténticos, será sancionado con la pena de presidio menor en sus grados medio a máximo. Cuando la conducta descrita en el inciso anterior sea cometida por empleado público, abusando de su oficio, será castigado con la pena de presidio menor en su grado máximo a presidio mayor en su grado mínimo. **Artículo 6°. -** Receptación de datos informáticos. El que conociendo su origen o no pudiendo menos que conocerlo comercialice, transfiera o almacene con el mismo objeto u otro fin ilícito, a cualquier título, datos informáticos, provenientes de la realización de las conductas descritas en los artículos 2°, 3° y 5°, sufrirá la pena asignada a los respectivos delitos, rebajada en un grado. **Artículo 7°. -** Fraude informático. El que, causando perjuicio a otro, con la finalidad de obtener un beneficio económico para sí o para un tercero, manipule un sistema informático, mediante la introducción, alteración, daño o supresión de datos informáticos o a través de cualquier interferencia en el funcionamiento de un sistema informático, será penado:

		1) Con presidio menor en sus grados medio a máximo y multa de once a quince unidades tributarias mensuales, si el valor del perjuicio excediera de cuarenta unidades tributarias mensuales. 2) Con presidio menor en su grado medio y multa de seis a diez unidades tributarias mensuales, si el valor del perjuicio excediere de cuatro unidades tributarias mensuales y no pasare de cuarenta unidades tributarias mensuales. 3) Con presidio menor en su grado mínimo y multa de cinco a diez unidades tributarias mensuales, si el valor del perjuicio no excediere de cuatro unidades tributarias mensuales. Si el valor del perjuicio excediere de cuatrocientas unidades tributarias mensuales, se aplicará la pena de presidio menor en su grado máximo y multa de veintiuna a treinta unidades tributarias mensuales. Para los efectos de este artículo se considerará también autor al que, conociendo o no pudiendo menos que conocer la ilicitud de la conducta descrita en el inciso primero, facilita los medios con que se comete el delito. **Artículo 8º.-** Abuso de los dispositivos. El que para la perpetración de los delitos previstos en los artículos 1° a 4° de esta ley o de las conductas señaladas en el artículo 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. **Artículo 9°. -** Derogado. **Artículo 10.-** Circunstancias agravantes. Constituyen circunstancias agravantes de los delitos de que trata esta ley: 1) Cometer el delito abusando de una posición de confianza en la administración del sistema informático o custodio de los datos informáticos contenidos en él, en razón del ejercicio de un cargo o función. 2) Cometer el delito abusando de la vulnerabilidad, confianza o desconocimiento de niños, niñas, adolescentes o adultos mayores. Asimismo, si como resultado de la comisión de las conductas contempladas en este Título, se afectase o interrumpiese la provisión o prestación de servicios de utilidad pública, tales como electricidad, gas, agua, transporte, telecomunicaciones o financieros, o el normal desenvolvimiento de los procesos electorales regulados en la ley Nº 18.700, orgánica constit**ucional sobre votaciones** populares y escrutinios, la pena correspondiente se aumentará en un grado. (…).

	Ley 19696 Establece Código Procesal Penal	**Artículo 218 bis. -** Preservación provisoria de datos informáticos. El Ministerio Público con ocasión de una investigación penal podrá requerir, a cualquier proveedor de servicio, la conservación o protección de datos informáticos o informaciones concretas incluidas en un sistema informático, que se encuentren a su disposición hasta que se obtenga la respectiva autorización judicial para su entrega. Los datos se conservarán durante un período de 90 días, prorrogable una sola vez, hasta que se autorice la entrega o se cumplan 180 días. La empresa requerida estará obligada a prestar su colaboración y guardar secreto del desarrollo de esta diligencia. **Artículo 218 ter. -** Registros de llamadas y otros antecedentes de tráfico comunicacional. Cuando existan fundadas sospechas basadas en hechos determinados y ello sea útil para la investigación, el Ministerio Público podrá requerir a cualquier proveedor de servicios, previa autorización judicial, que entregue la información que tenga almacenada relativa al tráfico de llamadas telefónicas, de envíos de correspondencia o de tráfico de datos en internet de sus abonados, referida al período de tiempo determinado en la resolución judicial. Ley 21577 Para efectos de este artículo se entenderá por datos relativos al tráfico todos aquellos referidos a una comunicación realizada por medio de un sistema informático o de telecomunicaciones, generados por este último en tanto elemento de la cadena de comunicación, y que indiquen el origen, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente. El Ministerio Público podrá requerir, en el marco de una investigación penal en curso y sin autorización judicial, a cualquier proveedor de servicios que ofrezca servicios en territorio chileno, que facilite los datos de suscriptor que posea sobre sus abonados, así como también la información referente a las direcciones IP utilizadas por éstos para facilitar la identificación de quienes corresponda en el marco de la investigación. Los proveedores de servicios deberán mantener el secreto de esta solicitud. Por datos de suscriptor se entenderá aquella información que posea un proveedor de servicios relacionada con sus abonados, excluidos los datos sobre tráfico y contenido, y que permita determinar su identidad, tales como la información del nombre del titular del servicio, número de identificación, domicilio, número de teléfono y correo electrónico. Las empresas concesionarias de servicios públicos de telecomunicaciones y proveedores de internet deberán mantener, con carácter reservado y adoptando las medidas de seguridad correspondientes, a disposición del Ministerio Público a efectos de una investigación penal, por un plazo de un año, una nómina y registro actualizado de sus rangos autorizados de direcciones IP y de los números IP de las conexiones que realicen sus clientes o usuarios, con sus correspondientes datos relativos al tráfico, así como los domicilios o residencias de sus clientes o usuarios. Los funcionarios públicos, los intervinientes en la investigación penal y los empleados de las empresas mencionadas en este artículo que intervengan en este tipo de requerimientos deberán guardar secreto acerca de ellos, salvo que se les cite a declarar. La entrega de los antecedentes deberá realizarse en el plazo que disponga la resolución judicial. Si el requerido estima que no puede cumplir con el plazo en atención al volumen y la naturaleza de la información solicitada o la información no existe o no la posee, deberá comunicar dicha circunstancia fundadamente al tribunal, dentro del término señalado en la resolución judicial respectiva. Si a pesar de las medidas señaladas en este artículo la información no es entregada, podrá ser requerida al representante legal de la institución u organización de que se trate, bajo apercibimiento de arresto.

		La infracción a la mantención de la nómina y registro actualizado de los antecedentes a que se refiere el inciso cuarto será castigada según las sanciones y el procedimiento previsto en los artículos 36 y 36 A de la ley N° 18.168, General de Telecomunicaciones. El incumplimiento de las obligaciones de mantener con carácter reservado y adoptar las medidas de seguridad correspondientes de los antecedentes señalados en dicho inciso, será sancionado con la pena prevista en la letra f) del artículo 36 B de la ley N° 18.168. Los registros así obtenidos quedarán bajo custodia del Ministerio Público, quien cuidará que los datos en cuestión no sean conocidos por terceras personas. Los registros sólo podrán ser utilizados para los efectos de la investigación en la que fueron solicitados, u otras seguidas por delitos que merezcan pena de crimen o sean propias del sistema de análisis criminal y focos investigativos, de acuerdo con lo establecido en el artículo 37 bis de la ley N° 19.640, que establece la ley orgánica constitucional del Ministerio Público, y no podrán ser utilizados para otros fines. El ejercicio de esta facultad se regulará mediante instrucciones generales dictadas por el Fiscal Nacional, conforme a lo establecido en el artículo 17 letra a) de la ley N° 19.640, con el objeto de asegurar su uso racional. **Artículo 219.-** Copias de comunicaciones o transmisiones. El juez de garantía podrá autorizar, a petición del fiscal, que cualquier empresa de comunicaciones facilite copias de las comunicaciones transmitidas o recibidas por ellas. Del mismo modo, podrá ordenar la entrega de las versiones que existieren de las transmisiones de radio, televisión u otros medios. (…). **Artículo 225 bis.** - Registro remoto de equipos informáticos y ámbito de aplicación. A petición fundada del Ministerio Público, el juez de garantía podrá autorizar la utilización de programas computacionales, contraseñas, códigos de seguridad o de acceso u otros datos similares, que permitan acceder de manera remota y aprehender el contenido de un dispositivo, computador o sistema informático, sin conocimiento de su usuario, cuando existan fundadas sospechas basadas en hechos determinados, de que una persona ha cometido o participado en la preparación o comisión, o que el delito se esté cometiendo actualmente, o que se esté preparando la comisión o participación en una asociación delictiva o criminal. La medida será autorizada por un plazo máximo de 8 días. El juez de garantía podrá prorrogar este plazo por períodos de hasta igual duración, con un máximo de días, para lo cual deberá examinar cada vez la Artículo segundo concurrencia de los requisitos previstos en el inciso anterior. **Artículo 225 ter. -** Requisitos de la resolución que autoriza la medida. La resolución judicial que autorice el acceso remoto deberá especificar, a solicitud del fiscal: a) Los dispositivos, computadores o sistemas informáticos específicos objeto de la medida y las circunstancias necesarias para individualizar o determinar al afectado por la medida. b) El alcance de la medida, la forma en la que se procederá al acceso y aprehensión de contenidos relevantes para la causa y el programa computacional software mediante el cual se realizará acceso remoto.

		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 contenidos para la causa. e) Las medidas técnicas específicas necesarias para preservar la integridad de los contenidos, así como para impedir el acceso y la supresión de dichos datos del sistema informático objeto de la medida. f) La duración precisa de la medida. **Artículo 225 quáter. -** Ampliación del registro. Cuando al ejecutarse el acceso remoto surjan motivos para creer que los contenidos buscados están almacenados en otro sistema informático o en una parte de él, el juez de garantía, a petición fundada del Ministerio Público, podrá autorizar la ampliación de los términos del acceso remoto. La resolución judicial que autorice la ampliación del registro deberá especificar los antecedentes señalados en el artículo anterior, que resulten pertinentes para el desarrollo de la ampliación. **Artículo 225 quinquies. -** Deber de colaboración. Los prestadores de servicios de telecomunicaciones, de acceso a una red de telecomunicaciones o de servicios de la sociedad de la información y los titulares o responsables del sistema informático o contenido objeto del acceso remoto, están obligados a colaborar con los funcionarios policiales encargados de ejecutar la medida. Asimismo, están obligados a facilitar la asistencia necesaria para que los contenidos aprehendidos puedan ser objeto de examen y visualización. Los sujetos requeridos para prestar la colaboración en este tipo de requerimientos deberán guardar secreto acerca de los mismos, salvo que se les cite a declarar. La ejecución de la técnica de investigación, en los términos de la resolución judicial que la autoriza, no podrá ser objeto de sanción penal o civil. (…).
Ecuador	Constitución de la República del Ecuador	**Art. 66.-** Se reconoce y garantizará a las personas: (…). 19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley. (…).

		Art. 92.- Toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico. Asimismo tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos. Las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la ley. La persona titular de los datos podrá solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación. En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias. Si no se atendiera su solicitud, ésta podrá acudir a la jueza o juez. La persona afectada podrá demandar por los perjuicios ocasionados. (…). **Art. 387.-** Será responsabilidad del Estado: (…). 3. Asegurar la difusión y el acceso a los conocimientos científicos y tecnológicos, el usufructo de sus descubrimientos y hallazgos en el marco de lo establecido en la Constitución y la Ley.
	Código Orgánico Integral Penal	**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 un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible. 2. La persona que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder. 3. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares. 4. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior.

		Art. 231.- Transferencia electrónica de activo patrimonial. - La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero, será sancionada con pena privativa de libertad de tres a cinco años. Con igual pena, será sancionada la persona que facilite o proporcione datos de su cuenta bancaria con la intención de obtener, recibir o captar de forma ilegítima un activo patrimonial a través de una transferencia electrónica producto de este delito para sí mismo o para otra persona. **Artículo 232.- Ataque a la integridad de sistemas informáticos. -** La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años. Con igual pena será sancionada la persona que: 1. Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo. 2. Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general. 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. (…). **Art. 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.-** La persona que sin autorización acceda en 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, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años. **Art. 476.- Interceptación de las comunicaciones o datos informáticos. -** La o el juzgador ordenará la interceptación de las comunicaciones o datos informáticos previa solicitud fundamentada de la o el fiscal cuando existan indicios que resulten relevantes a los fines de la investigación, de conformidad con las siguientes reglas:

		1. La o el juzgador determinará la comunicación interceptada y el tiempo de intercepción, que no podrá ser mayor a un plazo de noventa días. Transcurrido el tiempo autorizado se podrá solicitar motivadamente por una sola vez una prórroga hasta por un plazo de noventa días. Cuando sean investigaciones de delincuencia organizada y sus delitos relacionados, la interceptación podrá realizarse hasta por un plazo de seis meses. Transcurrido el tiempo autorizado se podrá solicitar motivadamente por una sola vez una prórroga hasta por un plazo de seis meses. 2. La información relacionada con la infracción que se obtenga de las comunicaciones que se intercepten durante la investigación serán utilizadas en el proceso para el cual se las autoriza y con la obligación de guardar secreto de los asuntos ajenos al hecho que motive su examen. 3. Cuando, en el transcurso de una interceptación se conozca del cometimiento de otra infracción, se comunicará inmediatamente a la o al fiscal para el inicio de la investigación correspondiente. En el caso de delitos flagrantes, se procederá conforme con lo establecido en este Código. 4. Previa autorización de la o el juzgador, la o el fiscal, realizará la interceptación y registro de los datos informáticos en transmisión a través de los servicios de telecomunicaciones como: telefonía fija, satelital, móvil e inalámbrica, con sus servicios de llamadas de voz, mensajes SMS, mensajes MMS, transmisión de datos y voz sobre IP, correo electrónico, redes sociales, videoconferencias, multimedia, entre otros, cuando la o el fiscal lo considere indispensable para comprobar la existencia de una infracción o la responsabilidad de los partícipes. 5. Está prohibida la interceptación de cualquier comunicación protegida por el derecho a preservar el secreto profesional y religioso. Las actuaciones procesales que violenten esta garantía carecen de eficacia probatoria, sin perjuicio de las respectivas sanciones. 6. Al proceso solo se introducirá de manera textual la transcripción de aquellas conversaciones o parte de ellas que se estimen útiles o relevantes para los fines de la investigación. No obstante, la persona procesada podrá solicitar la audición de todas sus grabaciones, cuando lo considere apropiado para su defensa. 7. El personal de las prestadoras de servicios de telecomunicaciones, así como las personas encargadas de interceptar, grabar y transcribir las comunicaciones o datos informáticos tendrán la obligación de guardar reserva sobre su contenido, salvo cuando se las llame a declarar en juicio. 8. El medio de almacenamiento de la información obtenida durante la interceptación deberá ser conservado por la o el fiscal en un centro de acopio especializado para el efecto, hasta que sea presentado en juicio. 9. Quedan prohibidas la interceptación, grabación y transcripción de comunicaciones que vulneren los derechos de los niños, niñas y adolescentes, especialmente en aquellos casos que generen la revictimización en infracciones de violencia contra la mujer o miembros del núcleo familiar, sexual, física, sicológica y otros. **Art. 477.- Reconocimiento de grabaciones. -** La o el juzgador autorizará a la o al fiscal el reconocimiento de las grabaciones mencionadas en el artículo anterior, así como de vídeos, datos informáticos, fotografías, discos u otros medios análogos o digitales. Para este efecto, con la

		intervención de dos peritos que juren guardar reserva, la o el fiscal, en audiencia privada, procederá a la exhibición de la película o a escuchar el disco o la grabación y a examinar el contenido de los registros informáticos. Las partes podrán asistir con el mismo juramento. La o el fiscal podrá ordenar la identificación de voces grabadas, por parte de personas que afirmen poder reconocerlas, sin perjuicio de ordenar el reconocimiento por medios técnicos. (…). **Art. 500.- Contenido digital. -** El contenido digital es todo acto informático que representa hechos, información o conceptos de la realidad, almacenados, procesados o transmitidos por cualquier medio tecnológico que se preste a tratamiento informático, incluidos los programas diseñados para un equipo tecnológico aislado, interconectado o relacionados entre sí. En la investigación se seguirán las siguientes reglas: 1. El análisis, valoración, recuperación y presentación del contenido digital almacenado en dispositivos o sistemas informáticos se realizará a través de técnicas digitales forenses. 2. Cuando el contenido digital se encuentre almacenado en sistemas y memorias volátiles o equipos tecnológicos que formen parte de la infraestructura critica del sector público o privado, se realizará su recolección, en el lugar y en tiempo real, con técnicas digitales forenses para preservar su integridad, se aplicará la cadena de custodia y se facilitará su posterior valoración y análisis de contenido. 3. Cuando el contenido digital se encuentre almacenado en medios no volátiles, se realizará su recolección, con técnicas digitales forenses para preservar su integridad, se aplicará la cadena de custodia y se facilitará su posterior valoración y análisis de contenido. 4. Cuando se recolecte cualquier medio físico que almacene, procese o transmita contenido digital durante una investigación, registro o allanamiento, se deberá identificar e inventariar cada objeto individualmente, fijará su ubicación física con fotografías y un plano del lugar, se protegerá a través de técnicas digitales forenses y se trasladará mediante cadena de custodia a un centro de acopio especializado para este efecto.
	Ley Orgánica de Protección de Datos Personales	**Art. 1.-**Objeto y finalidad. -El objeto y finalidad de la presente ley es garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre información y datos de este carácter, así como su correspondiente protección, Para dicho efecto regula, prevé y desarrolla principios, derechos, obligaciones y mecanismos de tutela. (…). **Art. 9.-**Interés legítimo. -Cuando el tratamiento de datos personales tiene como fundamento el interés legítimo: a) Únicamente podrán ser tratados los datos que sean estrictamente necesarios para la realización de la finalidad.

		b) El responsable debe garantizar que el tratamiento sea transparente para el titular. c) La Autoridad de Protección de Datos puede requerir al responsable un informe con de riesgo para la protección de datos en el cual se verificará si no hay amenazas concretas a las expectativas legítimas de los titulares y a sus derechos fundamentales. (…). **Art. 44.-**Acceso a datos personales para atención a emergencias e incidentes informáticos.-Las autoridades públicas competentes, los equipos de respuesta de emergencias informáticas, los equipos de respuesta a incidentes de seguridad informática, los centros de operaciones de seguridad, los prestadores y proveedores de servicios de telecomunicaciones y los proveedores de tecnología y servicios de seguridad, nacionales e internacionales, podrán acceder y efectuar tratamientos sobre los datos personales contenidos en las notificaciones de vulneración a las seguridades, durante el tiempo necesario, exclusivamente para la detección, análisis, protección y respuesta ante cualquier tipo de incidentes así como para adoptar e implementar medidas de seguridad adecuadas y proporcionadas a los riesgos identificados. (…). **Art. 47.-**Obligaciones del responsable y encargado del tratamiento de datos personales. -El responsable del tratamiento de datos personales está obligado a: 1) Tratar datos personales en estricto apego a los principios y derechos desarrollados en la presente Ley, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales, o normativa sobre la materia; 2) Aplicar e implementar requisitos y herramientas administrativas, técnicas, físicas, organizativas y jurídicas apropiadas, a fin de garantizar y demostrar que el tratamiento de datos personales se ha realizado conforme a lo previsto en la presente Ley, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales, o normativa sobre la materia; 3) Aplicar e implementar procesos de verificación, evaluación, valoración periódica de la eficiencia, eficacia y efectividad de los requisitos y herramientas administrativas, Técnicas, físicas, organizativas y jurídicas implementadas; 4) Implementar políticas de protección de datos personales afines al tratamiento de datos personales en cada caso en particular; 5) Utilizar metodologías de análisis y gestión de riesgos adaptadas a las particularidades del tratamiento y de las partes involucradas; 6) Realizar evaluaciones de adecuación al nivel de seguridad previas al tratamiento de datos personales;

		7) Tomar medidas tecnológicas, físicas, administrativas, organizativas y jurídicas necesarias para prevenir, impedir, reducir, mitigar y controlar los riesgos y las vulneraciones identificadas; 8) Notificar a la Autoridad de Protección de Datos Personales y al titular de los datos acerca de violaciones a las seguridades implementadas para el tratamiento de datos personales conforme a lo establecido en el procedimiento previsto para el efecto; 9) Implementar la protección de datos personales desde el diseño y por defecto; 10) Suscribir contratos de confidencialidad y manejo adecuado de datos personales con el encargado y el personal a cargo del tratamiento de datos personales o que tenga conocimiento de los datos personales; 11) Asegurar que el encargado del tratamiento de datos personales ofrezca mecanismos suficientes para garantizar el derecho a la protección de datos personales conforme a lo establecido en la presente ley, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales, normativa sobre la materia y las mejores prácticas a nivel nacional o internacional; 12) Registrar y mantener actualizado el Registro Nacional de Protección de Datos Personales, de conformidad a lo dispuesto en la presente Ley, en su reglamento, en directrices, lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales; 13) Designar al Delegado de Protección de Datos Personales, en los casos que corresponda; 14) Permitir y contribuir a la realización de auditorías o inspecciones, por parte de un auditor acreditado por la Autoridad de Protección de Datos Personales; y, 15) Los demás establecidos en la presente Ley en su reglamento, en directrices, lineamientos, regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativa sobre la materia. El encargado de tratamiento de datos personales tendrá las mismas obligaciones que el responsable de tratamiento de datos personales, en lo que sea aplicable, de acuerdo a la presente ley y su reglamento. (…). **Art. 51.-**Registro Nacional de protección de datos personales. -El responsable del tratamiento de datos personales deberá reportar y mantener actualizada la información ante la Autoridad de Protección de Datos Personales, sobre lo siguiente: 1) Identificación de la base de datos o del tratamiento; 2) El nombre domicilio legal y datos de contacto del responsable y encargado del tratamiento de datos personales;

		3) Características y finalidad del tratamiento de datos personales; 4) Naturaleza de los datos personales tratados; 5) Identificación, nombre, domicilio legal y datos de contacto de los destinatarios de los datos personales, incluyendo encargados y terceros; 6) Modo de interrelacionar la información registrada; 7) Medios utilizados para implementar los principios, derechos y obligaciones contenidas en la presente ley y normativa especializada; 8) Requisitos y herramientas administrativas técnicas y físicas, organizativas y jurídicas implementadas para garantizar la seguridad y protección de datos personales; 9) Tiempo de conservación de los datos. (…). **Art. 71.-**Sanciones por infracciones leves. -La Autoridad de Protección de Datos Personales impondrá las siguientes sanciones administrativas, en el caso de verificarse el cometimiento de una infracción leve, según las siguientes reglas: 1. Servidores o funcionarios del sector público por cuya acción u omisión hayan incurrido en alguna de las infracciones leves establecidas en la presente ley, serán sancionados con una multa de uno (1) a diez (10) salarios básicos unificados del trabajador en general, sin perjuicio de la responsabilidad extracontractual del Estado, la cual se sujetará a las reglas establecidas en la normativa correspondiente; 2. Si el responsable o el encargado del tratamiento de datos personales o de ser el caso un tercero es una entidad de derecho privado o una empresa pública, se aplicará una multa de entre el 0.1% y el 0.7% calculada sobre su volumen de negocio correspondiente al ejercicio económico inmediatamente anterior al de la imposición de la multa. La Autoridad de Protección de Datos Personales establecerá la multa aplicable en función del principio de proporcionalidad, para lo cual deberá verificar los siguientes presupuestos: a) La intencionalidad, misma que se establecerá en función a la conducta del infractor; b) Reiteración de la infracción, es decir cuando el responsable, el encargado del tratamiento de datos personales o de ser el caso un tercero, hubiese sido previamente sancionado por dos o más infracciones precedentes, que establezcan sanciones de menor gravedad a la que se pretende aplicar; o cuando hubiesen sido previamente sancionados por una infracción cuya sanción sea de igual o mayor gravedad a la que se pretende aplicar;

		c) La naturaleza del perjuicio ocasionado, es decir, las consecuencias lesivas para el ejercicio del derecho a la protección de datos personales; y, d) Reincidencia, es decir, cuando la infracción precedente sea de la misma naturaleza de aquella que se pretende sancionar. **Art. 72.-**Sanciones por infracciones graves. -La Autoridad de Protección de Datos Personales impondrán las siguientes sanciones administrativas, en el caso de verificarse el cometimiento de una infracción grave, conforme a los presupuestos establecidos en el presente Capítulo: Los servidores o funcionarios del sector público por cuya acción u omisión hayan incurrido en alguna de las infracciones graves establecidas en la presente ley serán sancionados con una multa de entre 10 a 20 salarios básicos unificados del trabajador en general; sin perjuicio de la Responsabilidad Extracontractual del Estado, la cual se sujetará a las reglas establecidas en la normativa correspondiente; 1) Si el responsable, encargado del tratamiento de datos personales o de ser el caso un tercero, es una entidad de derecho privado o una empresa pública se aplicará una multa de entre el 0.7% y el 1% calculada sobre su volumen de negocios, correspondiente al ejercicio económico inmediatamente anterior al de la imposición de la multa. La Autoridad de Protección de Datos Personales establecerá la multa aplicable en función del principio de proporcionalidad, para lo cual deberá verificar los siguientes presupuestos: a) La intencionalidad, misma que se establecerá en función a la conducta del infractor; b) Reiteración de la infracción, es decir, cuando el responsable, encargado del tratamiento de datos personales o de ser el caso, de un tercero hubiese sido previamente sancionado por dos o más infracciones precedentes que establezcan sanciones de menor gravedad a la que se pretende aplicar; o cuando hubiesen sido previamente sancionados por una infracción cuya sanción sea de igual o mayor gravedad a la que se pretende aplicar; c) La naturaleza del perjuicio ocasionado, es decir, las consecuencias lesivas para el ejercicio del derecho a la protección de datos personales; y, d) Reincidencia, es decir, cuando la infracción precedente sea de la misma naturaleza de aquella que se pretende sancionar. En el caso de que el responsable, encargado del tratamiento de datos personales a un tercero de ser el caso; sea una organización sin domicilio ni representación jurídica en el territorio ecuatoriano, se deberá notificar de la resolución con la cual se establezca la infracción cometida la Autoridad de Protección de Datos Personales, o quien hiciera sus veces, del lugar en donde dicha organización tiene su domicilio principal, a fin de que sea dicho organismo quien sustancia las acciones o procedimientos destinados al cumplimiento de las medidas correctivas y sanciones a las que hubiere lugar.
	Ley 67 Ley de Comercio Electrónico, Firmas y Mensajes de Datos	**Art. 1.-** Objeto de la ley. - Esta ley regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas.

		Art. 2.- Reconocimiento jurídico de los mensajes de datos. - Los mensajes de datos tendrán igual valor jurídico que los documentos escritos. Su eficacia, valoración y efectos se someterá al cumplimiento de lo establecido en esta ley y su reglamento. **Art. 3.-** Incorporación por remisión. - Se reconoce validez jurídica a la información no contenida directamente en un mensaje de datos, siempre que figure en el mismo, en forma de remisión o de anexo accesible mediante un enlace electrónico directo y su contenido sea conocido y aceptado expresamente por las partes. **Art. 4.-** Propiedad intelectual. - Los mensajes de datos estarán sometidos a las leyes, reglamentos y acuerdos internacionales relativos a la propiedad intelectual. **Art. 5.-** Confidencialidad y reserva. - Se establecen los principios de confidencialidad y reserva para los mensajes de datos, cualquiera sea su forma, medio o intención. Toda violación a estos principios, principalmente aquellas referidas a la intrusión electrónica, transferencia ilegal de mensajes de datos o violación del secreto profesional, será sancionada conforme a lo dispuesto en esta ley y demás normas que rigen la materia. **Art. 6.-** Información escrita. - Cuando la ley requiera u obligue que la información conste por escrito, este requisito quedará cumplido con un mensaje de datos, siempre que la información que este contenga sea accesible para su posterior consulta. **Art. 7**.- Información original.- Cuando la ley requiera u obligue que la información sea presentada o conservada en su forma original, este requisito quedará cumplido con un mensaje de datos, si siendo requerido conforme a la ley, puede comprobarse que ha conservado la integridad de la información a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos. Se considera que un mensaje de datos permanece integro, si se mantiene completo e inalterable su contenido, salvo algún cambio de forma, propio del proceso de comunicación, archivo o presentación. Por acuerdo de las partes y cumpliendo con todas las obligaciones previstas en esta ley, se podrán desmaterializar los documentos que por ley deban ser instrumentados físicamente. Los documentos desmaterializados deberán contener las firmas electrónicas correspondientes debidamente certificadas ante una de las entidades autorizadas según lo dispuesto en el artículo 29 de la presente ley, y deberán ser conservados conforme a lo establecido en el artículo siguiente. **Art. 8.-** Conservación de los mensajes de datos.- Toda información sometida a esta ley, podrá ser conservada; este requisito quedará cumplido mediante el archivo del mensaje de datos, siempre que se reúnan las siguientes condiciones: a. Que la información que contenga sea accesible para su posterior consulta;

		b. Que sea conservado con el formato en el que se haya generado, enviado o recibido, o con algún formato que sea demostrable que reproduce con exactitud la información generada, enviada o recibida; c. Que se conserve todo dato que permita determinar el origen, el destino del mensaje, la fecha y hora en que fue creado, generado, procesado, enviado, recibido y archivado; y, d. Que se garantice su integridad por el tiempo que se establezca en el reglamento a esta ley. Toda persona podrá cumplir con la conservación de mensajes de datos, usando los servicios de terceros, siempre que se cumplan las condiciones mencionadas en este artículo. La información que tenga por única finalidad facilitar el envío o recepción del mensaje de datos, no será obligatorio el cumplimiento de lo establecido en los literales anteriores. **Art. 9.-** Protección de datos.- Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros. La recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución Política de la República y esta ley, los cuales podrán ser utilizados o transferidos únicamente con autorización del titular u orden de autoridad competente. No será preciso el consentimiento para recopilar datos personales de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de la administración pública, en el ámbito de su competencia, y cuando se refieran a personas vinculadas por una relación de negocios, laboral, administrativa o contractual y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato. El consentimiento a que se refiere este artículo podrá ser revocado a criterio del titular de los datos; la revocatoria no tendrá en ningún caso efecto retroactivo. **Art. 10.-** Procedencia e identidad de un mensaje de datos. - Salvo prueba en contrario se entenderá que un mensaje de datos proviene de quien lo envía y, autoriza a quien lo recibe, para actuar conforme al contenido del mismo, cuando de su verificación exista concordancia entre la identificación del emisor y su firma electrónica, excepto en los siguientes casos: a) Si se hubiere dado aviso que el mensaje de datos no proviene de quien consta como emisor; en este caso, el aviso se lo hará antes de que la persona que lo recibe actúe conforme a dicho mensaje. En caso contrario, quien conste como emisor deberá justificar plenamente que el mensaje de datos no se inició por orden suya o que el mismo fue alterado; y,

		b) Si el destinatario no hubiere efectuado diligentemente las verificaciones correspondientes o hizo caso omiso de su resultado. **Art. 11.-** Envío y recepción de los mensajes de datos. - Salvo pacto en contrario, se presumirá que el tiempo y lugar de emisión y recepción del mensaje de datos, son los siguientes: a) Momento de emisión del mensaje de datos. - Cuando el mensaje de datos ingrese en un sistema de información o red electrónica que no esté bajo control del emisor o de la persona que envió el mensaje en nombre de éste o del dispositivo electrónico autorizado para el efecto; b) Momento de recepción del mensaje de datos. - Cuando el mensaje de datos ingrese al sistema de información o red electrónica señalado por el destinatario. Si el destinatario designa otro sistema de información o red electrónica, el momento de recepción se presumirá aquel en que se produzca la recuperación del mensaje de datos. De no haberse señalado un lugar preciso de recepción, se entenderá que ésta ocurre cuando el mensaje de datos ingresa a un sistema de información o red electrónica del destinatario, independientemente de haberse recuperado o no el mensaje de datos; y, c) Lugares de envío y recepción. - Los acordados por las partes, sus domicilios legales o los que consten en el certificado de firma electrónica, del emisor y del destinatario. Si no se los pudiere establecer por estos medios, se tendrán por tales, el lugar de trabajo, o donde desarrollen el giro principal de sus actividades o la actividad relacionada con el mensaje de datos. **Art. 12.-** Duplicación del mensaje de datos. - Cada mensaje de datos será considerado diferente. En caso de duda, las partes pedirán la confirmación del nuevo mensaje y tendrán la obligación de verificar técnicamente la autenticidad del mismo.
	Ley para prevenir y erradicar la violencia contra las mujeres	**Art. 12.-** Ámbitos donde se desarrolla la violencia contra las mujeres. Son los diferentes espacios y contextos en los que se desarrollan los tipos de violencia de género contra las mujeres: niñas, adolescentes, jóvenes, adultas y adultas mayores. Están comprendidos, entre otros, los siguientes: (…); 7. Mediático y cibernético. - Comprende el contexto en el que la violencia es ejercida a través de los medios de comunicación públicos, privados o comunitarios, sea por vía tradicional o por cualquier tecnología de la información, incluyendo las redes sociales, plataformas virtuales o cualquier otro; (…).
El Salvador	Constitución de la República	**Art. 24.-** La correspondencia de toda clase es inviolable, interceptada no hará fe ni podrá figurar en ninguna actuación, salvo en los casos de concurso y quiebra.

		Se prohíbe la interferencia y la intervención de las telecomunicaciones. de manera excepcional podrá autorizarse judicialmente, de forma escrita y motivada, la intervención temporal de cualquier tipo de telecomunicaciones, preservándose en todo caso el secreto de lo privado que no guarde relación con el proceso. la información proveniente de una intervención ilegal carecerá de valor. La violación comprobada a lo dispuesto en este artículo, por parte de cualquier funcionario, será causa justa para la destitución inmediata de su cargo y dará lugar a la indemnización por los daños y perjuicios ocasionados. Una ley especial determinará los delitos en cuya investigación podrá concederse esta autorización. asimismo señalará los controles, los informes periódicos a la asamblea legislativa, y las responsabilidades y sanciones administrativas, civiles y penales en que incurrirán los funcionarios que apliquen ilegalmente esta medida excepcional. la aprobación y reforma de esta ley especial requerirá el voto favorable de por lo menos las dos terceras partes de los diputados electos. (24)
	Decreto 260 Ley Especial contra los Delitos Informáticos y Conexos	**Objeto de la Ley** **Art. 1.-** La presente Ley tiene por objeto proteger los bienes jurídicos de aquellas conductas delictivas cometidas por medio de las Tecnologías de la Información y la Comunicación, así como la prevención y sanción de los delitos cometidos en perjuicio de los datos almacenados, procesados o transferidos; los sistemas, su infraestructura o cualquiera de sus componentes, o los cometidos mediante el uso de dichas tecnologías que afecten intereses asociados a la identidad, propiedad, intimidad e imagen de las personas naturales o jurídicas en los términos aplicables y previstos en la presente Ley. (…). **Definiciones** **Art. 3.-** Para los efectos de la presente Ley, se entenderá por: a) Delito Informático: se considerará la comisión de este delito, cuando se haga uso de las Tecnologías de la Información y la Comunicación, teniendo por objeto la realización de la conducta típica y antijurídica para la obtención, manipulación o perjuicio de la información; b) Bien Jurídico Protegido: es la información que garantice y proteja el ejercicio de derechos fundamentales como la intimidad, honor, integridad sexual, propiedad, propiedad intelectual, seguridad pública, entre otros; c) Datos Informáticos: es cualquier representación de hechos, información o conceptos en un formato digital o análogos, que puedan ser almacenados, procesados o transmitidos en un sistema informático, cualquiera que sea su ubicación, así como las características y especificaciones que permiten describir, identificar, descubrir, valorar y administrar los datos; d) Medio de Almacenamiento de Datos Informáticos: es cualquier dispositivo a partir del cual la información es capaz de ser leída, grabada, reproducida o transmitida con o sin la ayuda de cualquier otro medio idóneo;

		e) Sistema Informático: es un elemento o grupo de elementos interconectados o relacionados, pudiendo ser electrónicos, programas informáticos, enlaces de comunicación o la tecnología que en el futuro los reemplace, orientados al tratamiento y administración de datos e información; f) Comunicación Electrónica: es toda transmisión de datos informáticos, cuyo contenido puede consistir en audio, texto, imágenes, videos, caracteres alfanuméricos, signos, graficos de diversa índole o cualquier otra forma de expresión equivalente, entre un remitente y un destinatario a través de un sistema informático y las demás relacionadas con las Tecnologías de la Información y la Comunicación; g) Dispositivo: es cualquier mecanismo, instrumento, aparato, medio que se utiliza o puede ser utilizado para ejecutar cualquier función de la Tecnología de la Información y la Comunicación; h) Interceptar: es la acción de apropiarse, interrumpir, escuchar o grabar datos informáticos contenidos o transmitidos en cualquier medio informático antes de llegar a su destino; i) Programa Informático: es la rutina o secuencia de instrucciones en un lenguaje informático determinado que se ejecuta en un sistema informático, pudiendo ser éste un ordenador, servidor o cualquier dispositivo, con el propósito que realice el procesamiento y comunicación de los datos informáticos; j) Proveedor de Servicios: es la persona natural o jurídica que ofrece uno o más servicios de información o comunicación por medio de sistemas informáticos, procesamiento o almacenamiento de datos; k) Tráfico de Datos Informáticos: son aquellos que se transmiten por cualquier medio tecnológico, pudiendo mostrar el origen, destino, ruta, hora, fecha, tamaño, duración de la comunicación, entre otros; l) Tecnologías de la Información y la Comunicación: es el conjunto de tecnologías que permiten el tratamiento, la comunicación de los datos, el registro, presentación, creación, administración, modificación, manejo, movimiento, control, visualización, distribución, intercambio, transmisión o recepción de información en forma automática, de voz, imágenes y datos contenidos en señales de naturaleza acústica, óptica o electromagnética, entre otros; m) Datos Personales: es la información privada concerniente a una persona, identificada o identificable, relativa a su nacionalidad, domicilio, patrimonio, dirección electrónica, número telefónico u otra similar; n) Datos Personales Sensibles: son los que corresponden a una persona en lo referente al credo, religión, origen étnico, filiación o ideologías políticas, afiliación sindical, preferencias sexuales, salud física y mental, situación moral, familiar y otras informaciones íntimas de similar naturaleza o que pudieran afectar el derecho al honor, a la propia imagen, a la intimidad personal y familiar;

		o) Material Pornográfico de Niñas, Niños y Adolescentes: es toda representación auditiva o visual, ya sea en imagen o en vídeo, adoptando un comportamiento sexualmente explícito, real o simulado de una persona que aparente ser niña, niño o adolescente adoptando tal comportamiento. También se considerará material pornográfico, las imágenes realistas que representen a una niña, niño o adolescente adoptando un comportamiento sexualmente explícito o las imágenes reales o simuladas de las partes genitales o desnudos de una niña, niño o adolescente con fines sexuales; p) Tarjeta Inteligente: es el dispositivo que permite mediante la ejecución de un programa la obtención de bienes, servicios, propiedades o información; y, q) Redes Sociales: es la estructura o comunidad virtual que hace uso de medios tecnológicos y de la comunicación para acceder, establecer y mantener algún tipo de vínculo o relación, mediante el intercambio de información. r) Código Malicioso: Todo programa o conjunto de instrucciones en un lenguaje de programación que ejecuta el programa y que es diseñado para causar algún tipo de perjuicio; (1) s) Virus Informático: Es un programa malicioso que tiene por objetivo alterar el normal funcionamiento de un ordenador, equipo, dispositivo o su información; (1) t) Personas con Discapacidad: Son todas aquellas personas que tengan deficiencias físicas, psicosociales, intelectuales o sensoriales a largo plazo que, al interactuar con diversas barreras, puedan ver impedida o reducida su participación plena y efectiva en todos los ámbitos de la sociedad y que le generen mayor riesgo de padecer abusos tanto de carácter sexual, físico o psicológico; (1) u) Seducción: Conjunto de conductas que tienen como finalidad establecer una relación de intimidad para obtener un contacto de índole sexual. (1) TÍTULO II DE LOS DELITOS. CAPÍTULO I DE LOS DELITOS CONTRA LOS SISTEMAS TECNOLÓGICOS DE INFORMACIÓN. **Acceso Indebido a Sistemas Informáticos.** **Art. 4.-** El que intencionalmente y sin autorización o excediendo la que se le hubiere concedido, acceda, intercepte o utilice parcial o totalmente un sistema informático que utilice las Tecnologías de la Información o la Comunicación, será sancionado con prisión de uno a cuatro años. **Acceso Indebido a los Programas o Datos Informáticos.** **Art. 5.-** El que a sabiendas y con la intención de usar cualquier dispositivo de la Tecnología de la Información o la Comunicación, accediera parcial o totalmente a cualquier programa o a los datos almacenados en él, con el propósito de apropiarse de ellos o cometer otro delito con éstos, será sancionado con prisión de dos a cuatro años. Interferencia del Sistema Informático.

		Art. 6.- El que intencionalmente y por cualquier medio interfiera o altere el funcionamiento de un sistema o programa informático, de forma temporal o permanente, será sancionado con prisión de tres a seis años. (1) Se considerará agravada la interferencia o alteración, si ésta recayera en programas o sistemas informáticos públicos o en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión y transporte de energía, de medios de transporte u otros de servicio público, o destinados a la prestación de servicios financieros, o la realización de transacciones en Bitcoin u otras criptomonedas que permitan su convertibilidad automática e instantánea a moneda de curso legal, en estos casos la sanción de prisión será de cuatro a siete años. (1) **Daños a Sistemas Informáticos.** **Art. 7.-** El que destruya, dañe, modifique, ejecute un programa o realice cualquier acto que afecte el funcionamiento, o inhabilite parcial o totalmente un sistema o programa informático que utilice las Tecnologías de la Información y la Comunicación o cualquiera de los componentes que las conforman, será sancionado con prisión de tres a seis años. (1) Si el delito previsto en el presente artículo se cometiere en contra de cualquiera de los componentes de un sistema o programa informático que utilicen las Tecnologías de la Información y la Comunicación, que estén destinadas a la prestación de servicios públicos o financieros o la realización de transacciones en Bitcoin u otras criptomonedas que permitan su convertibilidad automática e instantánea a moneda de curso legal, o que contengan información personal, confidencial, reservada, patrimonial, técnica o propia de personas naturales o jurídicas, será sancionado con prisión de cuatro a siete años. (1) Si el delito previsto en el presente artículo se ejecutare por imprudencia, será sancionado con prisión de uno a tres años. (1) **Posesión y uso de Equipos o Prestación de Servicios para la Vulneración de la Seguridad** (1) **Art. 8.-** El que posea, produzca, facilite, venda equipos, dispositivos, programas informáticos, códigos maliciosos, virus informáticos, contraseñas o códigos de acceso; que utilicen las Tecnologías de la Información y la Comunicación, con el propósito de vulnerar, eliminar ilegítimamente la seguridad de cualquier sistema o programa informático, ofrezca servicios destinados a cumplir los mismos fines para cometer cualquiera de los delitos establecidos en la presente Ley, será sancionado con prisión de tres a cinco años. (1) Si el cometimiento delictivo se hiciere mediante el uso de los equipos, dispositivos, programas informáticos, códigos maliciosos, virus informáticos, contraseñas o códigos de acceso, aun cuando no se haya logrado la finalidad de eliminar ilegítimamente la seguridad informática, será sancionado con prisión de uno a tres años. (1) **Violación de la Seguridad del Sistema.** **Art. 9.-** La persona que sin poseer la autorización correspondiente transgreda la seguridad de un sistema informático restringido o protegido con mecanismo de seguridad específico, será sancionado con prisión de tres a seis años.

		En igual sanción incurrirá quien induzca a un tercero para que de forma involuntaria, ejecute un programa, mensaje, instrucciones o secuencias para violar medidas de seguridad. No incurrirá en sanción alguna quien ejecute las conductas descritas en los Arts. 8 y 9 inciso primero de la presente Ley, cuando con autorización de la persona facultada se realicen acciones con el objeto de conducir pruebas técnicas o auditorías de funcionamiento de equipos, procesos o programas. CAPÍTULO II DE LOS DELITOS INFORMÁTICOS. **Estafa informática.** **Art. 10.-** El que manipule o influya en el ingreso, el procesamiento o resultado de los datos de un sistema que utilice las Tecnologías de la Información y la Comunicación, ya sea mediante el uso de datos falsos o incompletos, el uso indebido de datos o programación, valiéndose de alguna operación informática o artificio tecnológico o por cualquier otra acción que incida en el procesamiento de los datos del sistema o que dé como resultado información falsa, incompleta o fraudulenta, con la cual procure u obtenga un beneficio patrimonial indebido para sí o para otro, en perjuicio patrimonial ajeno, será sancionado con prisión de cinco a ocho años. (1) Se sancionará con prisión de ocho a diez años, si las conductas descritas en el inciso anterior se cometieren bajo los siguientes presupuestos: (1) a) En perjuicio de propiedades del Estado; (1) b) Contra sistemas bancarios y entidades financieras, y se vieren o no afectados usuarios de los mismos; y, (1) c) Cuando el autor sea un empleado encargado de administrar, dar soporte al sistema, red informática, telemática o que en razón de sus funciones tenga acceso a dicho sistema, red, contenedores electrónicos, ópticos o magnéticos. (1) **Fraude Informático.** **Art. 11.-** El que por medio del uso indebido de las Tecnologías de la Información y la Comunicación, valiéndose de cualquier manipulación en sistemas informáticos o cualquiera de sus componentes, datos informáticos o información en ellos contenida, consiga insertar instrucciones falsas o fraudulentas que produzcan un resultado que permita obtener un provecho para sí o para un tercero en perjuicio ajeno, será sancionado con prisión de seis a diez años. (1) Si las conductas descritas en el inciso anterior se realizaran contra sistemas bancarios y entidades financieras o si afectan a usuarios de tales entidades; si afectaren la realización de transacciones de Bitcoin u otras criptomonedas o afecten sistemas que permitan su convertibilidad

		automática e instantánea a moneda de curso legal; y cuando el autor sea un empleado encargado de administrar, dar soporte al sistema, red informática, telemática o que en razón de sus funciones tenga acceso a dicho sistema, red, contenedores electrónicos, ópticos o magnéticos, será sancionado con prisión de diez a doce años. (1) **Falsedad de Documentos y Firmas** (1) **Art 11-A.-** Quien falsifique, desencripte, descodifique o de cualquier modo descifre, divulgue o trafique, con documentos, firmas, certificados, sean digitales, digitalizados o electrónicos, de registros públicos o privados, será sancionado con prisión de tres a seis años. (1) **Espionaje Informático.** **Art. 12.-** El que con fines indebidos obtenga datos, información reservada o confidencial contenidas en un sistema que utilice las Tecnologías de la Información y la Comunicación o en cualquiera de sus componentes, será sancionado con prisión de cinco a ocho años. Si alguna de las conductas descritas en el inciso anterior se cometieren con el fin de obtener beneficio para sí o para otro, se pusiere en peligro la seguridad del Estado, la confiabilidad de la operación de las instituciones afectadas, resultare algún daño para las personas naturales o jurídicas como consecuencia de la revelación de la información de carácter reservada, confidencial o sujeta a secreto bancario, la sanción será de seis a diez años de prisión. **Hurto por Medios Informáticos.** **Art. 13.-** El que, por medio del uso de las Tecnologías de la Información y la Comunicación, se apodere de bienes o valores tangibles o intangibles de carácter personal o patrimonial, sustrayéndolos a su propietario, tenedor o poseedor, con el fin de obtener un provecho económico para sí o para otro, será sancionado con prisión de cinco a ocho años. (1) Quien facilitare o dispusiera de cuenta electrónica, tarjetas de crédito o cualquier otro servicio financiero que permita trasladar, desviar u ocultar la transacción que regula el inciso anterior, será sancionado con prisión de dos a cinco años. (1) **Técnicas de Denegación de Servicio.** **Art. 14.-** El que de manera intencionada, utilizando las técnicas de la denegación de servicio o prácticas equivalentes que afectaren a los usuarios que tienen pertenencia en el sistema o red afectada, imposibilite obtener el servicio, será sancionado con prisión de tres a cinco años. CAPÍTULO III DELITOS INFORMÁTICOS RELACIONADOS CON EL CONTENIDO DE LOS DATOS. **Manipulación de Registros.** **Art. 15.-** Los Administradores de las Plataformas Tecnológicas de instituciones públicas o privadas, que deshabiliten, alteren, oculten, destruyan, o inutilicen en todo o en parte cualquier información, dato contenido en un registro de acceso, uso de los componentes de éstos, será sancionado con prisión de cinco a ocho años.

		Si las conductas descritas en el inciso anterior, favorecieren la comisión de otro delito, la sanción se agravará hasta en una tercera parte del máximo señalado. **Manipulación Fraudulenta de Tarjetas Inteligentes o Instrumentos Similares.** **Art. 16.-** El que intencionalmente y sin la debida autorización por cualquier medio cree, capture, grabe, copie, altere, duplique, clone o elimine datos informáticos contenidos en una tarjeta inteligente o en cualquier instrumento destinado a los mismos fines; con el objeto de incorporar, modificar usuarios, cuentas, registros, consumos no reconocidos, la configuración actual de éstos o de los datos en el sistema, será sancionado con prisión de cinco a ocho años. En la misma pena incurrirá quien, sin haber tomado parte en los hechos anteriores adquiera, comercialice, posea, distribuya, venda, realice cualquier tipo de intermediación de tarjetas inteligentes o instrumentos destinados al mismo fin o de datos informáticos contenidos en ellos o en un sistema. **Obtención Indebida de bienes o servicios por medio de Tarjetas Inteligentes o Medios Similares.** **Art. 17.-** El que sin autorización utilice una tarjeta inteligente ajena o instrumento destinado a los mismos fines, utilice indebidamente las Tecnologías de la Información y la Comunicación para la obtención de cualquier bien o servicio, realice cualquier tipo de pago sin erogar o asumir obligación alguna por la contraprestación obtenida, será sancionado con prisión de tres a ocho años. **Provisión Indebida de Bienes o Servicios.** **Art. 18.-** El que sin justificación, a través de un sistema informático utilice tarjetas inteligentes o instrumentos similares destinados a los mismos fines, cuya vigencia haya caducado o haya sido revocada por la institución que la emitió, o que se haya obtenido con el fin de suplantar la identidad contenida en dichas tarjetas inteligentes, será sancionado con prisión de cinco a ocho años. El que falsifique o altere los datos de las tarjetas inteligentes o instrumentos similares, con el fin de proveer a quien los presente, dinero, bienes o servicios, o cualquier otro objeto de valor económico, la sanción aumentará hasta una tercera parte del máximo de la pena prevista en el inciso anterior. **Alteración, Daño a la Integridad y Disponibilidad de los Datos.** **Art. 19.-** El que violando la seguridad de un sistema informático destruya, altere, duplique, inutilice o dañe la información, datos o procesos, en cuanto a su integridad, disponibilidad y confidencialidad en cualquiera de sus estados de ingreso, procesamiento, transmisión o almacenamiento, será sancionado con prisión de tres a seis años. **Interferencia de Datos.** **Art. 20.-** El que interfiera, obstruya o interrumpa el uso legítimo de datos o los produzca nocivos e ineficaces, para alterar o destruir los datos de un tercero, será sancionado con prisión de tres a seis años.

		Si alguna de las conductas descritas en el inciso anterior recae sobre datos, documentos, programas o sistemas informáticos públicos o sobre datos destinados a la prestación de servicios de salud, de comunicaciones, sistemas bancarios, entidades financieras, de provisión y transporte de energía, de medios de transporte u otro servicio público, la sanción de prisión será de cinco a ocho años. **Interceptación de Trasmisiones entre Sistemas de las Tecnologías de la Información y la Comunicación.** **Art. 21.-** La persona que sin justificación intercepte por medios tecnológicos cualquier transmisión hacia, desde o dentro de un sistema informático que no está disponible al público; o las emisiones electromagnéticas que están llevando datos de un sistema informático, será sancionada con prisión de siete a diez años. **Hurto de Identidad.** **Art. 22.-** El que suplantare o se apoderare de la identidad de una persona natural o jurídica por medio de las Tecnologías de la Información y la Comunicación, será sancionado con prisión de tres a cinco años. (1) Si con la conducta descrita en el inciso anterior se daña, extorsiona, defrauda, injuria o amenaza a otra persona para ocasionar perjuicio u obtener beneficios para sí mismo o para terceros y el apoderamiento recae sobre datos personales, datos sensibles, o datos confidenciales, definidos así por disposición legal o reglamentaria, o por acuerdo de voluntades entre personas naturales o jurídicas, será sancionado con prisión de cinco a ocho años. (1) Si con el comportamiento del inciso anterior los datos obtenidos, lo fueron, con ánimo de lucro para sí o para un tercero, la pena de prisión será de seis a diez años. (1) **Obtención y Divulgación No Autorizada** (1) **Art. 23.- El** que sin autorización obtenga o dé a conocer por medio de las Tecnologías de la Información o Comunicación, un código, contraseña de acceso o cualquier otro medio de acceder a un programa o datos almacenados en un equipo o dispositivo tecnológico, con el fin de lucrarse así mismo, a un tercero o para cometer un delito, será sancionado con prisión de cinco a ocho años. (1) Igual sanción tendrá el que sin autorización revele o difunda los datos o información, contenidos en un sistema informático que utilice las Tecnologías de la Información y la Comunicación o en cualquiera de sus componentes, con el fin de obtener algún tipo de beneficio para sí o para otro. (1) **Utilización de Datos Personales.** **Art. 24.-** El que sin autorización utilice datos personales o datos personales sensibles a través del uso de las Tecnologías de la Información y la Comunicación, violando sistemas de confidencialidad y seguridad de datos, insertando o modificando los datos en perjuicio de un tercero, será sancionado con prisión de cuatro a seis años. (1)

		La sanción aumentará hasta en una tercera parte del máximo de la pena prevista en el inciso anterior a quien proporcione o revele a otro, datos informáticos personales o personales sensibles registrados en un archivo o en un banco de datos cuyo secreto o confidencialidad estuviere obligado a preservar. (1) La persona natural o jurídica responsable del almacenamiento y cuido de los datos informáticos, responderá culposamente por la falta de control en el personal que incurriera en el inciso anterior, o por la falta de implementación de sistemas de seguridad informáticos que posibilitaron la extracción y uso, cuya sanción será de uno a tres años de prisión. (1) **Obtención y Transferencia de Información de Carácter Confidencial.** **Art. 25.-** El que deliberadamente obtenga o transfiera mediante el uso de las Tecnologías de la Información y la Comunicación, información de carácter confidencial, definida así por disposición legal o reglamentaria, o por acuerdo de voluntades entre personas naturales o jurídicas, sin el consentimiento de los titulares de esa información, será sancionado con prisión de cinco a ocho años. (1) **Revelación Indebida de Datos o Información de Carácter Personal.** **Art. 26.-** El que sin el consentimiento del titular de la información de carácter privado y personal revele, difunda o ceda en todo o en parte, dicha información o datos a los que se refiere el presente artículo, sean éstos en imágenes, video, texto, audio u otros, obtenidos por alguno de los medios indicados en los artículos precedentes, será sancionado con prisión de tres a cinco años. Si alguna de las conductas descritas en el inciso anterior, se hubiese realizado con ánimo de lucro, la comisión de otro delito o se difunda material sexual explícito en perjuicio de un tercero, será sancionado con prisión de cuatro a ocho años. Se impondrá el límite máximo de la pena del inciso anterior, aumentado hasta en una tercera parte, si alguna de las conductas descritas en el inciso primero del presente artículo, recae sobre datos personales confidenciales o sensibles definidos en la Ley de Acceso a la Información Pública. **Secuestro de Sistemas, Programas o Datos Informáticos** (1) **Art. 26-A.-** Quien por cualquier medio telemático accediere a sistemas de programas, o dispositivos electrónicos o datos informáticos de una persona natural o jurídica, restringiendo el acceso a ellos y a los datos informáticos almacenados, con el propósito de exigir u obtener un provecho a cambio de la liberación de estos, será sancionado con prisión de cuatro a seis años. (1) Si la conducta del inciso anterior afectare a sistemas, programas o datos informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión y transporte de energía, de medios de transporte u otros de servicio público, o destinados a la prestación de servicios financieros, o la realización de transacciones en Bitcoin u otras criptomonedas, así como que permitan su convertibilidad automática e instantánea a moneda de curso legal, la sanción de prisión será de seis a ocho años. (1) **Acoso a través de Tecnologías de la Información y la Comunicación.**

		Art. 27.- El que realice conducta sexual indeseada por quien la recibe, que implique frases, señas u otra conducta inequívoca de naturaleza o contenido sexual, por medio del uso de las Tecnologías de la Información y la Comunicación, será sancionado con prisión de cuatro a seis años. CAPÍTULO IV DELITOS INFORMÁTICOS CONTRA NIÑAS, NIÑOS Y ADOLESCENTES O PERSONAS CON DISCAPACIDAD. **Pornografía a través del Uso de Tecnologías de Información y la Comunicación.** **Art. 28.-** El que por cualquier medio que involucre el uso de las Tecnologías de la Información y la Comunicación fabrique, transfiriera, difunda, distribuya, alquile, venda, ofrezca, produzca, ejecute, exhiba o muestre material pornográfico, sexual entre niñas, niños y adolescentes o personas con discapacidad, será sancionado con prisión de cuatro a ocho años. Quien no advierta de forma visible el contenido del material pornográfico o sexual que se transmita mediante el uso de las Tecnologías de la Información y la Comunicación, no apto para niñas, niños, adolescentes o personas con discapacidad, será sancionado con prisión de tres a cinco años. **Seducción de niñas, niños y adolescente o personas con discapacidad por medio de las tecnologías de la información y la comunicación** (1) **Art. 28-A.-** El que mediante el uso de las Tecnologías de la Información y la Comunicación establezca o entable una relación con una niña, niño, adolescente o persona con discapacidad, con la finalidad de sostener un contacto de índole sexual, mediante esas tecnologías, o en persona, será sancionado con prisión de uno a tres años. (1) Intercambio de mensajes de contenido sexual con niñas, niños y adolescentes o personas con discapacidad por medio de las tecnologías de la información y la comunicación (1) Art. 28-B.- El que mediante el uso de las Tecnologías de la Información y la Comunicación envíe, solicite, intercambie o transmita con una niña, niño, adolescente o persona con discapacidad, audios, imágenes o videos de contenido sexual o sexualmente explícitas reales o simuladas, será sancionado con prisión de dos a cuatro años. (1) **Extorsión sexual de niñas, niños y adolescentes o personas con discapacidad por medio de las tecnologías de la información y la comunicación** (1) **Art. 28-C.-** El que obligue, chantajee, amenace o coaccione a una niña, niño, adolescente o persona con discapacidad, a enviar, remitir o trasmitir audios, imágenes o videos de contenido sexualmente explícito reales o simuladas, o de su cuerpo desnudo, con el propósito de obtener satisfacción sexual o provecho, utilidad, beneficio o ventaja para sí o para un tercero, será sancionado con prisión de ocho a doce años. (1) Si la conducta del inciso anterior también se amenazare, si no cumpliere con sus demandas y exigencias de proporcionar más contenido, con ocasionar un daño a sus amigos o familiares, o solicitare cualquier cantidad de remuneración económica, a cambio de no compartir, difundir o publicar el contenido sexualmente explícito reales o simuladas que tiene en su poder, incluidas de su cuerpo desnudo, será sancionado con la pena máxima de prisión. (1)

		Utilización de Niñas, Niños, Adolescentes o Personas con Discapacidad en Pornografía a través del Uso de las Tecnologías de la Información y la Comunicación. **Art. 29.-** El que por cualquier medio que involucre el uso de las Tecnologías de la Información y la Comunicación produzca, reproduzca, distribuya, publique, importe, exporte, ofrezca, financie, venda, comercie o difunda de cualquier forma, imágenes, videos o exhiba en actividades sexuales, eróticas o inequívocas de naturaleza sexual, explícitas o no, reales o simuladas, o utilice la voz de niñas, niños, adolescentes o personas con discapacidad, será sancionado con prisión de ocho a doce años. Igual sanción se impondrá a quien por medio de las Tecnologías de la Información y la Comunicación organice o participe en espectáculos públicos o privados, en los que se hace participar a las personas señaladas en el inciso anterior, en acciones pornográficas o eróticas. **Adquisición o Posesión de Material Pornográfico de Niñas, Niños, Adolescentes o Personas con Discapacidad a través del Uso de las Tecnologías de la Información y la Comunicación.** **Art. 30.-** El que adquiera para sí o para un tercero a través de cualquier medio que involucre el uso de las Tecnologías de la Información y la Comunicación, o posea material pornográfico en el que se haya utilizado a una niña, niño, adolescente o persona con discapacidad o su imagen para su producción, será sancionado con prisión de dos a cinco años. Igual sanción se aplicará al que posea en dispositivos de almacenamiento de datos informáticos o a través de cualquier medio que involucre el uso de las Tecnologías de la Información y la Comunicación, material pornográfico en el que se haya utilizado a una niña, niño, adolescente o persona con discapacidad o su imagen para su producción. **Corrupción de Niñas, Niños, Adolescentes o Personas con Discapacidad a través del Uso de las Tecnologías de la Información y la Comunicación.** **Art. 31.-** El que mantenga, promueva o facilite la corrupción de una niña, niño, adolescente o persona con discapacidad con fines eróticos, pornográficos u obscenos, por medio de las Tecnologías de la Información y la Comunicación, aunque la niña, niño, adolescente o persona con discapacidad lo consienta, será sancionado con prisión de ocho a doce años. Igual sanción se impondrá a quien haga propuestas implícitas o explícitas para sostener encuentros de carácter sexual o erótico, o para la producción de pornografía a través del uso de las Tecnologías de la Información y la Comunicación para sí, para otro o para grupos, con una niña, niño, adolescente o persona con discapacidad. **Acoso a Niñas, Niños y Adolescentes o Personas con Discapacidad a través del Uso de las Tecnologías de la Información y la Comunicación.** **Art. 32.-** Quien atormente, hostigue, humille, insulte, denigre u otro tipo de conducta que afecte el normal desarrollo de la personalidad, amenace la estabilidad psicológica o emocional, ponga en riesgo la vida o la seguridad física, de un niño, niña, adolescente o persona con discapacidad, por medio del uso de las Tecnologías de la Información o Comunicación, será sancionado con prisión de dos a cuatro años.

		La pena se agravará con prisión de cuatro a ocho años, para quien realice conducta que implique frases, señas u otra acción inequívoca de naturaleza o contenido sexual contra una niña, niño, adolescente o persona con discapacidad, por medio del uso de las Tecnologías de la Información y la Comunicación. **Condiciones Agravantes Comunes.** **Art. 33.-** Los delitos referidos en el presente Capítulo, serán sancionados con la pena máxima correspondiente, aumentada hasta en una tercera parte del máximo establecido de la pena y la inhabilitación del ejercicio de su profesión durante el tiempo que dure la condena, si cualquiera de las acciones descritas fuera realizada por: a) Ascendientes, descendientes, hermanos, adoptantes, adoptados, cónyuges, conviviente y familiares hasta el cuarto grado de consanguinidad y segundo de afinidad; b) Funcionarios, empleados públicos y municipales, autoridad pública y agente de autoridad; c) La persona encargada de la tutela, protección o vigilancia de la víctima; y, d) Toda persona que prevaliéndose de la superioridad originada por relaciones de confianza, doméstica, educativa, de trabajo o cualquier otra relación. CAPÍTULO V DELITO CONTRA EL ORDEN ECONÓMICO. **Suplantación en actos de comercialización.** **Art. 34.-** El que sin autorización y a nombre de un tercero, mediante el uso de las Tecnologías de la Información y la Comunicación, venda o comercialice bienes o servicios, suplantando la identidad del productor, proveedor o distribuidor autorizado, será sancionado con prisión de tres a cinco años. La conducta descrita en el inciso anterior se agravará con pena de prisión de cuatro a seis años, cuando la venta o comercialización se trate de medicamentos, suplementos o productos alimenticios, bebidas o cualquier producto de consumo humano. (…).
	Decreto 144 Ley para la Protección de Datos Personales	Objeto Art. 1.- La presente ley tiene por objeto establecer la regulación para la protección de los datos personales, determinando los requisitos esenciales para realizar el tratamiento legítimo e informado de éstos y el marco normativo que debe seguirse en su recolección, uso, procesamiento,

		almacenamiento y otras actividades relacionadas a ellos; todo en aras de garantizar el derecho a la intimidad y a la autodeterminación informativa de las personas naturales. Principios rectores Art. 5.- Los principios rectores para la protección de datos son: a) Principio de la exactitud de los datos: los datos personales deberán mantenerse exactos, completos y actualizados hasta donde sea posible para las finalidades de su tratamiento, de tal manera que no se altere su veracidad. Se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan. Se presumirán exactos y actualizados los datos obtenidos directamente de su titular. b) Principio de lealtad: el responsable tratará los datos personales en su posesión, privilegiando la protección de los intereses de sus titulares y absteniéndose de tratar o recabar éstos a través de medios fraudulentos, desleales y/o ilícitos. c) Principio de consentimiento y finalidad: en el tratamiento y recolección de datos personales debe existir un consentimiento libre, especifico, informado, expreso e individualizado del titular, que establezca el fin, propósito y periodo de almacenamiento y tratamiento. d) Principio de minimización de datos: los datos personales recopilados y utilizados deben ser suficientes, pertinentes y no excesivos en relación con el propósito específico y legítimo. e) Principio de Transparencia: consiste en informar al titular de los datos personales de todas las características del tratamiento al que serán sometidos sus datos y, asimismo, exige que esa información se facilite en forma concisa, de fácil acceso y con un lenguaje claro y sencillo. Se prohíbe recurrir a textos extensos, terminologías técnicas o legales y/o letra pequeña en la aplicación de este principio. f) Principio de Seguridad de Datos: se refiere a garantizar la seguridad, integridad, disponibilidad y confidencialidad de los datos personales, a fin de evitar su alteración, pérdida, consulta o tratamiento no autorizado, así como detectar desviaciones de información, intencionales o no, que provengan de la acción humana o de un medio técnico. g) Principio de Licitud: El tratamiento de datos personales debe realizarse en cumplimiento a lo establecido en la presente ley y la normativa aplicable, para lo cual debe cumplirse al menos una de las siguientes condiciones: 1. El tratamiento de los datos se base en el consentimiento expreso otorgado por el titular para una o varias finalidades. 2. El tratamiento sea necesario para la ejecución de un contrato, del cual forma parte el titular, o para la ejecución de medidas precontractuales.

		3. El tratamiento sea necesario para el cumplimiento, por parte del responsable, de alguna obligación legal. 4. El tratamiento sea necesario para garantizar la protección de los intereses vitales del titular u otra persona afectada. 5. El tratamiento sea necesario para el cumplimiento de un fin de interés público o para que el responsable pueda ejercer los poderes públicos que le han sido conferidos. 6. El tratamiento sea necesario para que el responsable pueda satisfacer sus intereses legítimos, siempre y cuando esos intereses no atenten contra los derechos o libertades de los titulares de los datos personales. h) Principio de temporalidad: la conservación de los datos personales debe limitarse al periodo en el que se lograran los fines que se persiguen para su tratamiento. i) Principio de responsabilidad demostrada: una entidad que recoge y efectúa el tratamiento de datos personales debe ser responsable del cumplimiento efectivo de las medidas que implementen para proteger la privacidad de sus titulares y de garantizar una efectiva protección de datos personales. j) Principio de ejercicio progresivo de las facultades: Los derechos y garantías reconocidos a las niñas, niños y adolescentes serán ejercidos de manera progresiva tomando en consideración el desarrollo evolutivo de sus facultades, su condición o situación individual, la dirección y orientación apropiada de sus padres, madres o de quien ejerza la representación legal, y las disposiciones establecidas en la legislación vigente. CAPÍTULO III DERECHOS DE LOS TITULARES DE LOS DATOS PERSONALES Y SU EJERCICIO SECCIÓN A DERECHOS ARCO-POL **Derecho a la protección de los datos personales** **Art. 6.-** Toda persona, por sí mismo o por medio de su representante con facultades especiales, tendrá derecho a conocer si sus datos personales están siendo procesados para garantizar la protección de los mismos, cuando sea procedente podrá solicitar la rectificación, cancelación o bloqueo de éstos; a oponerse al tratamiento de sus datos; y, a solicitar que se limite su tratamiento en el futuro para usos distintos a los consentidos. Asimismo, tendrán derecho a obtener una reproducción inteligible de sus datos personales y a transferirlos cuando así lo consideren pertinente. Tratándose de los datos personales de personas fallecidas, le corresponderá a sus herederos o sucesores ejercer los derechos correspondientes, debiendo acreditar con documentación que demuestre su calidad de heredero o sucesor.

		Derecho de información frente a la recolección de datos **Art. 7.-** El titular de sus datos personales tendrá derecho a conocer quienes resguardarán éstos. Este derecho incluye también a los proveedores de servicios de almacenamiento tercerizados, como el encargado del tratamiento de datos personales que fue contratado por el responsable a tales efectos y que utiliza como medio de almacenamiento la nube u otra infraestructura. La información deberá ser almacenada en forma tal que se garantice plenamente el derecho de acceso por el titular de la misma. Asimismo, cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa, precisa e inequívoca, lo siguiente: a) El propósito o finalidad para la que serán recolectados y tratados, así como quiénes pueden ser sus destinatarios o clase de destinatarios. b) La existencia de la base de datos o repositorio, así como los respaldos y sitios de contingencia, en el caso que aplique. c) La identidad, domicilio, correo electrónico, número telefónico y cualquier información que facilite contactar al responsable y al encargado del tratamiento, o a sus respectivos representantes. d) El contenido de los derechos ARCO-POL y los mecanismos para ejercerlos. e) Las medidas y mecanismos de protección y seguridad que el responsable ha tomado y mantiene activas para salvaguardar la información. La información brindada de conformidad a los literales anteriores no tendrá costo alguno, y podrá ser proporcionada mediante la publicación de políticas de privacidad de forma física y/o electrónica, las que deben ser fácilmente accesibles e identificables. Cuando se proyecte un tratamiento de datos distinto de aquel para el cual se recolectaron, se proporcionará al titular información sobre esta finalidad ulterior y cualquier otra información adicional pertinente. El titular tendrá derecho de revocar la autorización otorgada inicialmente y deberá emitir una nueva autorización para que sus datos sean tratados conforme a la nueva finalidad. En todo caso, se deberá notificar a las partes, los efectos de proporcionarlos, de la negativa a hacerlo o de su inexactitud. **Derecho de acceso a datos personales** **Art. 8.-** El titular de datos personales tendrá derecho a obtener toda la información que sobre sí mismo se encuentre en bases de datos o registros físicos. Este derecho de acceso será ejercido en forma gratuita conforme a lo establecido en la presente ley. La información personal a la cual se concederá acceso deberá ser suministrada: a) En forma clara y exenta de codificaciones, la cual deberá ser acompañada de una explicación de los términos que se utilicen, los sujetos que han consultado dicha información y con qué propósito.

		b) De manera completa, siempre y cuando la misma no haya sido objeto de seudonimización o disociación, en cuyo caso se dejara constancia de dichas circunstancias. En ningún caso el informe podrá revelar datos pertenecientes a terceros, aun cuando se vinculen con el titular. Esta información podrá obtenerse mediante la mera consulta de su titular o su representante, previa identificación de su identidad y de los datos que por medio de su visualización pretende conocer, o también se podrá obtener con la indicación de los datos que son objeto de tratamiento por medios electrónicos o por cualquier otro medio que la tecnología permita y cuyo contenido sea legible e inteligible; esto sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos, imágenes o cualquier otro medio usado para dicho propósito. Adicionalmente, se debe comunicar si se ha realizado un intercambio de su información personal con otras instituciones o entidades. (…). TÍTULO II DE LAS ACTIVIDADES REALIZADAS SOBRE LOS DATOS PERSONALES CAPÍTULO I PRIVACIDAD DE LOS DATOS PERSONALES **Aviso de privacidad** **Art. 24.-** El aviso de privacidad es el documento físico, electrónico o digital mediante el cual el responsable, previo al tratamiento y recolección de datos, informa al titular sobre los términos bajo los cuales serán tratados sus datos personales. Este aviso deberá ser consistente con la política de privacidad que deberá elaborar el responsable para tal efecto. El contenido del aviso de privacidad tendrá, al menos, la siguiente información: a) El domicilio del responsable. b) Los datos personales que serán sometidos a tratamiento, identificando aquéllos que son sensibles. c) El fundamento legal que faculta al responsable para realizar el tratamiento. d) Las finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquéllas que requieren el consentimiento del titular. e) Los mecanismos, medios y procedimientos disponibles para ejercer los derechos ARCO-POL y los mecanismos para revocar el consentimiento. f) Indicación del nombre del delegado y lugar o medios para presentar la solicitud de derechos ARCO-POL.

		g) Los medios a través de los cuales el responsable comunicará a los titulares los cambios al aviso de privacidad. h) Los datos de contacto de la entidad subcontratada encargada del tratamiento de datos personales, en caso de existir. i) El uso de cookies. El aviso de privacidad podrá ser difundido por los medios físicos o electrónicos al titular de los datos personales, debiendo ser redactado y estructurado de manera clara y sencilla. En ningún caso el responsable podrá eximirse de la obligación de comunicarlo por escrito al titular al momento de que este otorgue su consentimiento informado para que sus datos puedan ser tratados. **Notificación de vulneraciones a la seguridad de los datos personales** **Art. 25.-** Cuando el responsable tenga conocimiento de una vulneración de seguridad de datos personales ocurrida en cualquier fase del tratamiento, entendiéndose ésta como cualquier daño, pérdida, alteración, destrucción, acceso ilegitimo, y en general, cualquier uso ilícito o no autorizado de los datos personales aun cuando ocurriera de manera accidental, notificará a la Agencia de Ciberseguridad del Estado, a la Fiscalía General de la República y a los titulares afectados dicho acontecimiento, para lo cual se establece un plazo máximo de setenta y dos horas desde que se tuvo conocimiento de la vulneración de seguridad. Dentro de este mismo plazo, el responsable deberá iniciar un proceso de revisión exhaustiva para determinar la magnitud de la afectación, y las medidas correctivas y preventivas que correspondan, así como la actualización de las políticas de seguridad del responsable de la base de datos para evitar nuevas vulneraciones La notificación que realice el responsable a la Entidad Rectora estará redactada en un lenguaje claro y sencillo y contendrá, al menos, la siguiente información: a) La naturaleza del incidente. b) Los datos personales comprometidos. c) Las acciones correctivas generales realizadas de forma inmediata. d) Las recomendaciones al titular sobre las medidas que éste pueda adoptar para proteger sus interese. e) Los medios disponibles al titular para obtener mayor información al respecto. La notificación dirigida a los titulares afectados únicamente deberá contener lo establecido en los literales a), b), d) y e).

		Asimismo, el responsable documentará toda vulneración ocurrida en cualquier fase del tratamiento que ocasione un riesgo en la seguridad de los datos personales, identificando de manera enunciativa más no limitativa, la fecha en que ocurrió, el motivo de la vulneración, los hechos relacionados con ella, sus efectos o implicaciones y las medidas correctivas implementadas de forma inmediata y definitiva, la cual estará a disposición de la autoridad encargada de la materia. (…). CAPÍTULO III DEL TRATAMIENTO DE DATOS PERSONALES **Tratamiento de datos personales Art. 32**.- El tratamiento de datos personales por parte de todos los responsables sólo podrá efectuarse respecto de los fines previamente informados y con sujeción a las normas aplicables. En el caso de las instituciones o empresa privada, únicamente deberá realizar el tratamiento de los datos personales que tengan relación directa con la naturaleza de los servicios que prestarán o prestaron al titular, en ningún caso podrán transferir o tratar datos personales de terceros para ofrecer otro tipo de servicios o cualquier finalidad diferente a la que éstos fueron recabados, sin previa autorización del titular. **Procedimientos para el ejercicio de los derechos ARCO-POL** **Art. 33.-** El responsable establecerá y documentará procedimientos para el ejercicio de los derechos ARCO-POL sobre los datos personales objetos de tratamiento, con base en las políticas de actuación emitidas por la Entidad Rectora y las medidas de seguridad mínimas necesarias. En los casos en el que el responsable subcontrate servicios en los cuales se conceda acceso a los datos personales, estos proveedores deberán someterse a la presente ley y a los lineamientos que el responsable y la Entidad Rectora establezca para garantizar el adecuado tratamiento de los datos personales. **Obligaciones para el tratamiento de datos personales** **Art. 34.-** El responsable, y en su caso el encargado del tratamiento de datos, además del cumplimiento de los principios establecidos en la presente ley, tendrá las obligaciones siguientes: a) Limitar el tratamiento de los datos personales de conformidad a la finalidad para la que se emitió el consentimiento por parte del titular. b) Implementar las medidas de seguridad y cumplir con las políticas de actuación conforme a la presente ley. c) Guardar confidencialidad en el tratamiento de los datos personales. d) Cualquier otra obligación que le atribuya la presente ley. **De las políticas de actuación y manejo de datos personales**

		Art. 35.- La Entidad Rectora dictará las políticas de actuación y manejo de datos personales, las cuales serán imperativas a los sujetos obligados por la presente ley. **De las medidas de seguridad en el tratamiento de datos personales** **Art. 36.- El** responsable deberá acatar y mantener las medidas de seguridad establecidas por la Entidad Rectora para el resguardo y el tratamiento de los datos personales y que garanticen el cumplimiento de las características mínimas de seguridad de la información, tales como integridad, disponibilidad y confidencialidad. El responsable deberá aplicar los mecanismos tecnológicos, regulatorios y procedimentales que garanticen el cumplimiento de las características de seguridad de información. Lo dispuesto en este artículo también será de obligatorio cumplimiento para el encargado del tratamiento de datos personales. (…).
Uruguay	Constitución de la República	Artículo 7º.- Los habitantes de la República tienen derecho a ser protegidos en el goce de su vida, honor, libertad, seguridad, trabajo y propiedad. Nadie puede ser privado de estos derechos sino conforme a las leyes que se establecen por razones de interés general.
	Ley 20.327 Tipificación de Ciberdelito	**Artículo 1°. -** Agréganse al Capítulo I del Título XI del Libro II del Código Penal, los siguientes artículos: "ARTÍCULO 288 BIS. (Acoso telemático).- El que, mediante la utilización de medios telemáticos, desarrolle de forma insistente cualquiera de las siguientes conductas será castigado con de tres meses de prisión a tres años de penitenciaría: vigilar, perseguir o procurar cercanía física, estableciendo o intentando establecer contacto con una persona, sea de forma directa o por intermedio de terceros, de tal modo que altere gravemente el desarrollo de su vida". "ARTÍCULO 288 TER. (Circunstancias agravantes especiales del delito de acoso telemático).- Será circunstancia agravante especial del delito de acoso telemático que se constituya en detrimento de un menor de edad, de adultos incapaces, de personas que previamente hayan tenido una relación afectiva o íntima, o de individuos vulnerables por enfermedad o por situaciones especiales que supongan una mayor fragilidad". **Artículo 2º.-** Agrégase al Capítulo IV del Título X del Libro II del Código Penal el siguiente artículo: "ARTÍCULO 277 TER. (Circunstancias agravantes especiales del delito previsto por el artículo 277 BIS). – A) Que las actividades descriptas en el tipo se ejecuten mediante coacción, intimidación o engaño hacia los menores de edad. B) Que el hecho sea realizado por personas con un vínculo de afinidad o parentesco con el menor de edad.

		C) Que el contacto se realice con un menor de trece años de edad con discapacidad, deficiencias físicas o psíquicas". **Artículo 3°. -** Agréganse al Capítulo III del Título XIII del Libro II del Código Penal los siguientes artículos: "ARTÍCULO 347 BIS. (Fraude informático).- Se considera autor de fraude informático y será castigado con la pena prevista en el artículo 347 quien incurra en alguna de las siguientes conductas: A) Inducir, con estratagemas o engaños artificiosos, induzca en error a alguna persona para obtener información mediante tecnologías de la información y de la comunicación para procurar, para sí mismo o un tercero, un provecho injusto en daño de otro. B) Efectuar manipulaciones informáticas o artificios afines con el fin de realizar operaciones financieras, transferencias o pagos no consentidos en perjuicio de otro, independientemente de que el beneficio sea personal o de un tercero. C) Utilizar cualquier tipo de tarjeta, cheque, código o cualquier otro medio de pago, o los datos vinculados a los mismos, para realizar transferencias, pagos o cualquier operación no consentida con el fin de obtener un provecho en daño de otro". "ARTÍCULO 348 BIS. (Circunstancias agravantes).- Serán circunstancias agravantes especiales del delito de fraude informático: A) Que exista parentesco o vinculación laboral o afectiva con la víctima o el tercero perjudicado. B) Que el hecho se efectúe en perjuicio del Estado o de cualquier ente público, o afecte infraestructuras críticas. C) Que el hecho se efectúe generando en la víctima el temor de un peligro imaginario o la persuasión de obedecer a una orden de la autoridad". **Artículo 4°. -** Agrégase al artículo 34 de la Ley Nº 19.574, de 20 de diciembre de 2017, el siguiente numeral: "34) Fraude informático cuyo monto real o estimado sea superior a 200.000 UI (doscientas mil unidades indexadas)". **Artículo 5°. -** Agréganse al Capítulo VI del Libro II del Título XIII del Código Penal, los siguientes artículos: "ARTÍCULO 358 QUATER. (Daño informático).- El que, por cualquier medio y sin autorización, destruya, altere o inutilice datos o sistemas informáticos con la finalidad de causar un daño será castigado de seis a veinticuatro meses de prisión". "ARTÍCULO 359 TER. - Serán circunstancias agravantes especiales del delito de daño informático: A) Que el daño ocasionado sea irreparable o sea imposible retornar a su estado anterior.

		B) Que el daño se cometa en perjuicio de documentos electrónicos o sistemas informáticos de carácter estatal o vinculados a infraestructuras críticas". **Artículo 6°. -** Agréganse al Capítulo III del Libro II del Título XI del Código Penal los siguientes artículos: "ARTÍCULO 297 BIS. (Acceso ilícito a datos informáticos).- El que mediante medios informáticos o telemáticos, sin autorización y sin justa causa acceda, interfiera, difunda, venda o ceda información ajena contenida en soporte digital, será castigado con seis a veinticuatro meses de prisión". "ARTÍCULO 297 TER. (Interceptación ilícita).- El que sin autorización y sin justa causa intercepte, interrumpa o interfiera por medios técnicos, datos informáticos en transmisiones no públicas, dirigidas a un sistema informático, sean originadas en un sistema informático o efectuadas dentro del mismo, incluyendo las emisiones electromagnéticas provenientes de un sistema informático que transporte los mismos, será castigado con seis a veinticuatro meses de prisión". "ARTÍCULO 297 QUATER. (Vulneración de datos).- El que mediante la utilización de cualquier medio telemático acceda, se apodere, utilice, o modifique datos confidenciales de terceros, registrados en soportes digitales, o cualquier otro tipo de archivo o registro público o privado, sin autorización de su titular, será castigado con seis a veinticuatro meses de prisión. El que, habiendo formado parte o no de su descubrimiento, difunda, revele o ceda a terceras personas los datos, hechos o imágenes registrados en soportes digitales será castigado con un año de prisión a cuatro años de penitenciaría. Constituye circunstancia agravante especial de este delito: A) Que sea cometido por personas encargadas de custodiar los soportes informáticos, electrónicos, registros o archivos digitales. B) Que el sujeto pasivo sea un menor de edad o un adulto declarado judicialmente incapaz. C) Que se cometa con una finalidad lucrativa. D) Que sea cometido en afectación de datos personales tutelados por la Ley N° 18.331, de 11 de agosto de 2008. E) Que se trate de datos estatales o vinculados a infraestructuras críticas". **Artículo 7°. -** Agréganse al Capítulo III del Título XIII del Libro II del Código Penal, los siguientes artículos: "ARTÍCULO 347 TER. (Suplantación de identidad).- El que usurpe, adopte, cree o se apropie de la identidad de otra persona física o jurídica, valiéndose de cualquier medio, herramienta tecnológica o sistema informático, obteniendo datos accediendo a redes sociales, casillas de correo

		electrónico, cuentas bancarias, medios de pago, plataformas digitales, o cualquier credencial digital o factor de autenticación, con la intención de dañar a su legítimo titular, será castigado con un año de prisión a seis años de penitenciaría. No constituirá suplantación de identidad la creación de nuevos perfiles destinados exclusivamente a la parodia". "ARTÍCULO 348 TER. (Circunstancias agravantes especiales).- Serán circunstancias agravantes especiales del delito de suplantación de identidad: A) Que se cometa con la finalidad de divulgar la información a la cual se accedió. B) Que se modifiquen, supriman o adulteren datos de la víctima o utilicen las credenciales para vincularse con terceras personas físicas o jurídicas. C) Que se adquieran, mediante el uso indebido de sus datos personales productos o mercaderías, o contraten servicios a través de medios telemáticos, en nombre de la víctima. D) Que se suplante la identidad de un organismo estatal u otro vinculado a infraestructuras críticas. E) La concurrencia con extorsión a la víctima, sus familiares o terceras personas vinculadas, para la obtención de activos o cualquier prestación en especie a los efectos de recuperar las referidas credenciales". **Artículo 8°. -** Agrégase al Capítulo VI del Título XIII del Libro II del Código Penal, el siguiente artículo: "Artículo 358 QUINQUIES. (Abuso de los dispositivos).- El que de forma ilegítima, produzca, adquiera, importe, comercialice o facilite a terceros, programas, sistemas informáticos o telemáticos de cualquier índole, credenciales o contraseñas de acceso a datos informáticos o sistemas de información, destinados inequívocamente a la comisión de un delito, será castigado con seis a veinticuatro meses de prisión". **Artículo 9°.-** (Campaña nacional educativa).- El Poder Ejecutivo promoverá una campaña nacional educativa sobre el manejo de finanzas personales y ciberseguridad en los centros educativos dependientes de la Dirección General de Educación Secundaria y de la Dirección General de Educación Técnico-Profesional de la Administración Nacional de Educación Pública, que deberá comprender, además, a beneficiarios de prestaciones servidas por el Banco de Previsión Social, Ceibal y los programas del Instituto Nacional de Empleo y Formación Profesional. Los conceptos a desarrollar deberán revisarse y actualizarse periódicamente acompasando los avances tecnológicos y serán los siguientes: A) Medios de pago, (dinero electrónico, diferencia entre subtipos de tarjetas, realización de operaciones en línea y cualquier otro medio de pago electrónico que pudiere desarrollarse).

		B) Cuentas bancarias: cajas de ahorro, cuentas corrientes, (diferencias entre ambas y vinculación a la Ley N° 19.210, de 29 de abril de 2014, y al Decreto-Ley N° 14.701, de 12 de setiembre de 1977). C) Acceso al financiamiento: préstamos (análisis de tasas de interés, plazos, cálculo de cuota contra ingresos mensuales, consecuencias de incumplimientos). D) Instituciones financieras: diferencia entre agentes clásicos y nuevos participantes, (plataformas de comercio electrónico y mensajería instantánea, entre otras). E) Planificación presupuestaria: relación ahorro y consumo, costo del dinero. F) Antecedentes crediticios: clearing de informes, central de riesgos del Banco Central del Uruguay, implicancias e impacto en acceso al crédito. G) Intangibilidad del salario (límite para el endeudamiento, pago de prestaciones alimenticias, orden de deducciones). H) Mecanismos de defensa al usuario financiero. I) Canales digitales y riesgos derivados de su uso inadecuado. J) Ejercicio de derechos en el entorno digital y aplicación de conceptos de autorregulación, comportamiento ético y empático en el ciberespacio. K) Fraudes tendientes al acceso de datos personales y financieros, que se determinan según las siguientes definiciones: 1) Phishing: suplantación de identidad, técnica de ingeniería social que usan los ciberdelincuentes para obtener información confidencial de los usuarios de forma fraudulenta y así apropiarse de la identidad de esas personas. 2) Vishing: tipo de estafa de ingeniería social por teléfono en la que a través de una llamada, se suplanta la identidad de una empresa, organización o persona de confianza, con el fin de obtener información personal y sensible de la víctima. 3) Smishing: técnica que consiste en el envío de un mensaje de texto por parte de un ciberdelincuente a un usuario simulando ser una entidad legítima (red social, banco, institución pública u otros) con el objetivo de robarle información privada o causarle un perjuicio económico. 4) Malware: hace referencia al software malicioso, que afecte los intereses del usuario, entendiéndose software al conjunto de programas y rutinas que permiten a una computadora realizar determinadas tareas.

		5) Troyano: es un programa que instala otros programas a menudo malware, sin consentimiento. 6) Ingeniería social: son las diferentes técnicas de manipulación que usan los ciberdelincuentes para obtener información confidencial de los usuarios, engañando a sus víctimas haciéndose pasar por otra persona. L) Buenas prácticas para el uso de canales digitales (riesgos asociados a su utilización por parte de menores de edad, relevancia de la supervisión). Asimismo, deberá asegurarse la igualdad en el acceso a las tecnologías de la información y de la comunicación, así como la equidad de género en su uso y acceso por lo que las entidades competentes deberán desarrollar campañas de seguridad digital en todo el territorio nacional con el fin de generar espacios de formación, capacitación, sociabilización y accesibilidad en las tecnologías de la información y la educación de forma equitativa a hombres y mujeres e igualitaria en materia de generaciones y discapacidad. **Artículo 10°. -** (Registro de antecedentes).- Facúltase a las instituciones de intermediación financiera y a las entidades emisoras de dinero electrónico a crear registros interinstitucionales que contengan datos para identificar, gestionar y prevenir transacciones no consentidas, operativas fraudulentas y tomar medidas preventivas conjuntas sobre los beneficiarios de éstas. A los solos efectos de compartir entre sí la información a que refiere el inciso anterior, no aplicarán a las instituciones y entidades mencionadas las limitaciones impuestas por el Decreto-Ley N° 15.322, de 17 de setiembre de 1982, quedando dichas instituciones y entidades facultadas para compartir sus registros con las autoridades jurisdiccionales, a los efectos de radicar denuncias y realizar gestiones tendientes a prevenir y mitigar los ciberdelitos tipificados en la presente ley. **Artículo 11°.-** (Inmovilización de fondos).- Facúltase a las instituciones de intermediación financiera y a las entidades emisoras de dinero electrónico a la no ejecución de cualquier tipo de orden de retiro o transferencia de activos brindada por personas físicas o jurídicas titulares o apoderados de cuentas, cuando hubieren tomado conocimiento, por cualquier medio de comunicación fehaciente, que en las cuentas referidas ingresaron fondos de terceros a través de transacciones que les fueran declaradas como desconocidas y no autorizadas por el titular de las cuentas de origen de los fondos transferidos. Lo dispuesto comprende instrucciones efectuadas directamente por los titulares de la cuenta así como instrucciones impartidas por sus representantes o apoderados a cualquier título. La inmovilización de fondos referida en el inciso anterior se aplicará a las cuentas correspondientes y comprenderá los saldos actuales e ingresos futuros de fondos o valores a dichas cuentas. En cualquier caso, la inmovilización de fondos alcanzará hasta el límite del monto de las transacciones denunciadas como desconocidas y no autorizadas por el titular de las cuentas de origen de los fondos transferidos, debiendo las instituciones de intermediación financiera y las entidades emisoras de dinero electrónico ejecutar toda orden que excediera dicho límite, salvo que las mismas no cumplan con requisitos legales o contractuales.

		La inmovilización de los fondos consecuentemente con lo dispuesto en los incisos anteriores, deberá ser comunicada dentro del plazo de un día hábil al Banco Central del Uruguay (BCU), quien podrá solicitar información adicional a las instituciones de intermediación financiera y a las entidades emisoras de dinero electrónico donde se encuentran radicadas las cuentas de origen y destino vinculadas a las transacciones denunciadas como desconocidas y no autorizadas y, previo análisis de la información a la que acceda, podrá instruir dejar sin efecto la inmovilización de fondos. La inmovilización de fondos deberá dejarse sin efecto y comunicarse al BCU cuando ocurra alguna de las siguientes situaciones: A) La institución de intermediación financiera o la entidad emisora de dinero electrónico donde se encuentra radicada la cuenta afectada no hubiere recibido dentro del plazo de cuarenta y ocho horas de efectuada la inmovilización, constancia de denuncia presentada por el titular de la cuenta origen de los fondos ante autoridad competente (Ministerio del Interior o Fiscalía General de la Nación). B) La institución de intermediación financiera o la entidad emisora de dinero electrónico donde se encuentra radicada la cuenta afectada no hubiere recibido, dentro del plazo de treinta días siguientes a la recepción de la constancia de denuncia referida en el literal A), una orden jurisdiccional confirmando la medida de inmovilización. C) La institución de intermediación financiera o la entidad emisora de dinero electrónico donde se encuentra radicada la cuenta afectada por inmovilización recibiera de cualquier autoridad jurisdiccional competente instrucción de dejar sin efecto la inmovilización referida. D) La institución de intermediación financiera o la entidad emisora de dinero electrónico donde se encuentra radicada la cuenta afectada por inmovilización recibiera, del titular de la misma, elementos de convicción suficiente o documentación fehaciente que, a su exclusivo criterio, indiquen que la transacción denunciada fue efectivamente autorizada por el titular de la cuenta de origen. Las instituciones de intermediación financiera y las entidades emisoras de dinero electrónico podrán radicar o ampliar denuncias ante las autoridades competentes, y realizar gestiones interinstitucionales, quedando facultadas para brindar todos los datos vinculados a las operaciones no consentidas.
	Ley 19.580 Violencia hacia las mujeres, basada en género	**Artículo 7º**.- (Derechos de las mujeres víctimas de violencia).- Además de los derechos reconocidos a todas las personas en la legislación vigente, nacional e internacional aplicable, toda mujer víctima de alguna de las formas de violencia basada en género, tiene derecho: (…). E) A que se garantice la confidencialidad y la privacidad de sus datos personales, los de sus descendientes o los de cualquiera otra persona que esté bajo su tenencia o cuidado. (…). **Artículo 11**.- (Instituto Nacional de las Mujeres).- El Instituto Nacional de las Mujeres es el órgano rector de las políticas públicas para una vida libre de violencia para las mujeres, responsable de la promoción, diseño, coordinación, articulación, seguimiento y evaluación de las mismas.

		En especial, debe: (…). J) Generar registros de datos cuantitativos y cualitativos sobre violencia basada en género, que contemplen variables tales como edad, situación de discapacidad, origen étnico racial, religión, territorialidad, entre otras dimensiones de la discriminación. Deberán adoptarse medidas a fin de garantizar la reserva de los datos personales de forma que no sea identificable la persona a la que refieren. (…). **Artículo 92**.- (Divulgación de imágenes o grabaciones con contenido íntimo).- El que difunda, revele exhiba o ceda a terceros imágenes o grabaciones de una persona con contenido íntimo o sexual, sin su autorización, será castigado con una pena de seis meses de prisión a dos años de penitenciaría. En ningún caso se considerará válida la autorización otorgada por una persona menor de dieciocho años de edad. Este delito se configura aun cuando el que difunda las imágenes o grabaciones haya participado en ellas. Los administradores de sitios de internet, portales, buscadores o similares que, notificados de la falta de autorización, no den de baja las imágenes de manera inmediata, serán sancionados con la misma pena prevista en este artículo. Artículo 93.- (Circunstancias agravantes especiales).- La pena prevista en el artículo anterior se elevará de un tercio a la mitad cuando: A) Las imágenes o grabaciones difundidas hayan sido obtenidas sin el consentimiento de la persona afectada. B) Se cometiera respecto al cónyuge, concubino o persona que esté o haya estado unida por análoga relación de afectividad, aun sin convivencia. C) La víctima fuera menor de dieciocho años de edad. D) La víctima fuera una persona en situación de discapacidad. E) Los hechos se hubieran cometido con una finalidad lucrativa. **Artículo 94.-** Incorpórese en el Código Penal el siguiente artículo: “ARTÍCULO 277 bis.- El que, mediante la utilización de tecnologías, de internet, de cualquier sistema informático o cualquier medio de comunicación o tecnología de trasmisión de datos, contactare a una persona menor de edad o ejerza influencia sobre el mismo, con el propósito de cometer cualquier delito contra su integridad sexual, actos con connotaciones sexuales, obtener material pornográfico u obligarlo a hacer o no hacer algo en contra de su voluntad será castigado con de seis meses de prisión a cuatro años de penitenciaría”.

Fuente: Páginas Web oficiales: Argentina, Bolivia, Colombia, Chile, Ecuador, El Salvador y Uruguay
Elaboración: Área de Servicios de Información y Seguimiento Presupuestal (ASISP)