DECRETO No. 260.-

LA ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE EL SALVADOR,

CONSIDERANDO:

I. Que la Constitución de la República, reconoce a la persona humana como el origen y el fin de la actividad del Estado, que está organizado para la consecusión de la justicia, de la seguridad jurídica y del bien común;

II. Que mediante Decreto Legislativo No. 1030, de fecha 26 de abril de 1997, publicado en el Diario Oficial No. 105, Tomo 335, del 10 de junio del mismo año, se emitió el Código Penal;

III. Que en la actualidad, los instrumentos electrónicos por medio de los cuales se envía, recibe o resguarda la información, han adquirido una especial relevancia, tanto a nivel internacional como nacional, para el desarrollo económico, político, social y cultural del país; por lo que se vuelve prioridad del Estado, proteger dicha información, ya que al no protegerla se atenta contra la confidencialidad, integridad, seguridad y disponibilidad de los datos en general; y,

IV. Que esta diversidad de actividades delincuenciales que pueden cometerse a través de las Tecnologías de la Información y la Comunicación, no se encuentran suficientemente reguladas en nuestra normativa penal vigente, generándose una impunidad para quienes cometen estos tipos de delitos; en consecuencia, resulta necesaria su tipificación y la adopción de mecanismos suficientes para facilitar su detección, investigación y sanción de estos nuevos tipos de delitos.

POR TANTO,

En uso de sus facultades constitucionales y a iniciativa del Diputado Douglas Leonardo Mejía Avilés, de los Períodos Legislativos 2009 - 2012 y 2012 - 2015.

DECRETA, la siguiente:

LEY ESPECIAL CONTRA LOS DELITOS INFORMÁTICOS Y CONEXOS.

TÍTULO I

DISPOSICIONES GENERALES.

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.

Ámbito de Aplicación.

Art. 2.- La presente Ley se aplicará a los hechos punibles cometidos total o parcialmente en el territorio nacional o en los lugares sometidos a su jurisdicción. También se aplicará a cualquier persona, natural o jurídica, nacional o extranjera, por delitos que afecten bienes jurídicos del Estado, de sus habitantes o protegidos por Pactos o Tratados Internacionales ratificados por El Salvador.

De igual forma, se aplicará la presente Ley si la ejecución del hecho, se inició en territorio extranjero y se consumó en territorio nacional o si se hubieren realizado, utilizando Tecnologías de la Información y la Comunicación instaladas en el territorio nacional y el responsable no ha sido juzgado por el mismo hecho por tribunales extranjeros o ha evadido el juzgamiento o la condena.

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;

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)

v) **Propietario de los Datos:** es la persona o entidad que tiene la propiedad principal sobre sus datos. Esto incluye la autoridad para exigir la implementación de políticas y procedimientos sobre cómo se manejan, almacenan y protegen sus datos. El Propietario de los datos tiene el derecho a que se garantice que sus datos sean precisos, accesibles y protegidos contra usos no autorizados. (2)

w) **Custodio de los Datos:** es la persona o entidad encargada de la gestión técnica y la protección de los datos. Esto incluye tareas como la implementación de medidas de seguridad, la administración de la infraestructura de almacenamiento de datos y el cumplimiento de las políticas y procedimientos exigidos por el Propietario de los Datos. El Custodio de los Datos asegura que estos se manejen de acuerdo con los estándares y regulaciones aplicables. (2)

x) **Controlador de los Datos:** es la persona o entidad que determina los propósitos y los medios para el procesamiento de datos personales. Esto implica decidir por qué y cómo se procesan los datos personales. El Controlador de los Datos tiene la responsabilidad principal de garantizar que el procesamiento de datos cumpla con los estándares y regulaciones aplicables. (2)

y) **Procesador de los Datos:** es la persona o entidad que procesa datos personales en nombre del Controlador de los Datos. Las actividades de procesamiento pueden incluir la recopilación,

almacenamiento, modificación o eliminación de datos personales. El Procesador de los Datos, posee además la calidad de custodio de los datos, por lo que, debe seguir las instrucciones del Controlador de los Datos y cumplir con las obligaciones contractuales y legales en relación con el manejo seguro y adecuado de los datos personales, así como los estándares y regulaciones aplicables. (2)

z) **Metadatos:** se definen como los datos que proporcionan información sobre uno o más aspectos de los datos; se utiliza para resumir información básica sobre datos que puede facilitar el seguimiento y el trabajo con datos específicos. (2)

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 mediante el uso indebido de las Tecnologías de la Información y la Comunicación, valiéndose de cualquier manipulación en sistemas informáticos, sus componentes, datos, metadatos, configuraciones o la información en ellos contenida, inserte instrucciones falsas o fraudulentas que resulten en un provecho para sí o para un tercero, en perjuicio ajeno, será sancionado con prisión de seis a diez años. (1) (2)

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)

Asimismo, será sancionado con prisión de diez a doce años, quien en razón de sus funciones, tenga acceso legitimo a un sistema informático, base de datos, sistemas de gestión de relaciones con clientes (CRM), sistemas y plataformas de ventas, servicios de centros de contacto, servicios basados en tecnologías blockchain, servicios de subcontratación de procesos de negocio, y sistemas o servicios donde los registros de información de terceros estén disponibles; con el fin de consultar, extraer o utilizar de manera ilegitima, registros de información de terceros, o para otorgar beneficios no autorizados, eliminar, ocultar o no documentar interacciones, realizar manipulaciones indebidas sobre los registros de información contenidos en dichos sistemas, o para crear información falsa a nombre del propietario de los datos, excediendo las autorizaciones otorgadas, con el fin de obtener un beneficio para sí o para un tercero, en perjuicio del propietario de los datos, del controlador o procesador de los mismos. (2)

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)

Si alguna de las conductas descritas en los incisos anteriores pusieren en peligro la seguridad del Estado, la confiabilidad de la operación de las instituciones afectadas o resultare algún daño para las personas naturales

o jurídicas, como consecuencia de la revelación de las informaciones de carácter reservado, será sancionado con prisión de seis a doce años.

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.

TÍTULO III

DISPOSICIONES FINALES.

Otras Responsabilidades.

Art. 35.- Las sanciones previstas en la presente Ley, serán aplicables sin perjuicio de otras responsabilidades penales, civiles o administrativas en que se incurra.

Para la deducción de la responsabilidad civil se estará a lo dispuesto en la normativa aplicable.

Especialización en la Investigación de los Delitos Informáticos (1)

Art. 35-A.- La Policía Nacional Civil y la Fiscalía General de la República deberán asegurar que el personal de investigaciones y los fiscales auxiliares cuenten con el conocimiento necesario y la actualización constante para la realización de sus atribuciones y el combate de los delitos informáticos contenidos en esta Ley y en otras Leyes Penales. (1)

Unidades de Investigación Científica de los Delitos Informáticos, Tratamiento y Análisis de la Evidencia Digital (1)

Art. 35-B.- La Policía Nacional Civil y la Fiscalía General de la República conforme a la organización que cada uno de los titulares de ellas determinen, podrán contar con Unidades de Investigación Científica de los Delitos Informáticos, Tratamiento y Análisis de la Evidencia Digital que permitan realizar las pericias de auditoria informática forense u otras que se requieran en la investigación de los hechos punibles contemplados en esta

Ley y en otras en que se dispongan delitos informáticos o se requiera el tratamiento y análisis de la evidencia digital; debiendo los titulares de cada una de las instituciones garantizar la organización institucional necesaria para tal fin y la coordinación entre ellas. (1)

Presupuestos institucionales (1)

Art. 35-C.- El Estado a través del Ministerio de Hacienda, deberá garantizar para la ejecución de la presente Ley por parte de la Policía Nacional Civil, Procuraduría General de la República y la Fiscalía General de la República, la asignación de partidas presupuestarias etiquetadas en el Presupuesto General de la Nación para cada año, las cuales deberán permitir la constante actualización de los equipos, de los sistemas o programas informáticos o pagos de licencias, la contratación de personal especializado y la capacitación y actualización constante de los mismos. (1)

Para efectos del inciso anterior, la Policía Nacional Civil, Procuraduría General de la República y la Fiscalía General de la República deberán indicarla al Ministerio de Hacienda, en su respectivo proyecto de presupuesto para cada ejercicio fiscal, sus necesidades institucionales para tal fin, y esta última cartera de Estado, deberá priorizar conforme lo permitan, los ingresos generales del Estado, la asignación de las partidas presupuestarias necesarias. (1)

Vigencia.

Art. 36.- El presente Decreto entrará en vigencia ocho días después de su publicación en el Diario Oficial.

DADO EN EL SALÓN AZUL DEL PALACIO LEGISLATIVO: San Salvador, a los cuatro días del mes de febrero del año dos mil dieciséis.

LORENA GUADALUPE PEÑA MENDOZA
PRESIDENTA

GUILLERMO ANTONIO GALLEGOS NAVARRETE
PRIMER VICEPRESIDENTE

ANA VILMA ALBANEZ DE ESCOBAR
SEGUNDA VICEPRESIDENTA

JOSÉ SERAFÍN ORANTES RODRÍGUEZ,
TERCER VICEPRESIDENTE

NORMAN NOEL QUIJANO GONZÁLEZ
CUARTO VICEPRESIDENTE

SANTIAGO FLORES ALFARO
QUINTO VICEPRESIDENTE

GUILLERMO FRANCISCO MATA BENNETT
PRIMER SECRETARIO

DAVID ERNESTO REYES MOLINA
SEGUNDO SECRETARIO

MARIO ALBERTO TENORIO GUERRERO
TERCER SECRETARIO

REYNALDO ANTONIO LÓPEZ CARDOZA
CUARTO SECRETARIO

JACKELINE NOEMÍ RIVERA ÁVALOS
QUINTA SECRETARIA

JORGE ALBERTO ESCOBAR BERNAL
SEXTO SECRETARIO

ABILIO ORESTES RODRÍGUEZ MENJÍVAR
SÉPTIMO SECRETARIO

JOSÉ FRANCISCO MERINO LÓPEZ
OCTAVO SECRETARIO

CASA PRESIDENCIAL: San Salvador, a los veintiséis días del mes de febrero del año dos mil dieciséis.

PUBLÍQUESE,

SALVADOR SÁNCHEZ CERÉN,
Presidente de la República.

MAURICIO ERNESTO RAMÍREZ LANDAVERDE,
Ministro de Justicia y Seguridad Pública.

REFORMAS:

(1) Decreto Legislativo No. 236 de fecha 07 de diciembre de 2021, publicado en el Diario Oficial No. 8, Tomo 434 de fecha 12 de enero de 2022.

(2) Decreto Legislativo No. 332 de fecha 19 de junio de 2025, publicado en el Diario Oficial No. 117, Tomo 447 de fecha 25 de junio de 2025.