GOBIERNO DE PUERTO RICO

19na. Asamblea Legislativa — 1ra. Sesión Ordinaria

SENADO DE PUERTO RICO

P. del S. 273

26 de marzo de 2020

Presentado por el señor *Ríos Santiago*

Referido a la Comisión de lo Jurídico

LEY

Para añadir un nuevo Libro Tercero - Ciberdelincuencia; eliminar los actuales Artículos 301, 302, 303, 304, 305, 306, 307, 308 y 309, para ser reenumerados bajo el nuevo Libro Tercero – Ciberdelincuencia de la Ley Núm. 146-2012, según enmendada, conocida como "Código Penal de Puerto Rico", a los fines de tipificar delitos cibernéticos y otros conexos de los mismos; y para otros fines relacionados.

EXPOSICIÓN DE MOTIVOS

Esta Asamblea Legislativa tiene la responsabilidad constitucional de salvaguardar la vida, propiedad y seguridad de todos los miembros de nuestra sociedad. En cumplimiento con dicha responsabilidad constitucional, corresponde tomar las medidas necesarias para prevenir, controlar y reducir la incidencia de la actividad criminal, incluyendo las conductas del mundo cibernético.

La aplicación de una pena sobre un individuo constituye una de las muestras más abarcadoras de la intensidad que puede asumir el castigo estatal. Esta afirmación se vuelve clara con solo pensar en el modo más usual en que una persona encontrada culpable de un delito es afectada con la pérdida de su libertad. Así, la detención o arresto de una persona para ser privada de su libertad se transforma en el ejemplo de la sanción penal. Desde luego existen otras penas que impactan sobre el patrimonio

(sanciones y multas) o en la capacidad para ejercer algún cargo, profesión o función. La gravedad de las penas en su aplicación debe estar prevista únicamente para aquellos actos específicos que el estado ha identificado y establecido mediante Ley. No obstante, la tarea de creación de delitos debe ser llevada a cabo con sumo cuidado, a fin de evitar vaguedad en su tipificación y/o el establecimiento de una punibilidad que resulte de manera excesiva o represiva por parte del estado.

La formulación de leyes penales es un proceso continuo que obedece a las condiciones sociales en determinado momento histórico. Según expresan las teorías de legislación penal, todo Código Penal debe ser el reflejo diáfano y genuino de los valores de la sociedad para la cual se legisla. De igual forma, no debemos perder de perspectiva que la creación de delitos va atada a ciertos principios fundamentales para una sociedad democrática. Así, toda tipificación de conducta delictiva, sanción y multa, deben ser realista, acorde con los tiempos que se viven y lo suficientemente abarcadora y flexible en miras de un futuro previsible o probable. Debe, además, ser susceptible de ajuste para atemperarlo a las situaciones cambiantes, según éstas acontecen.

Es por ello que, el debido proceso de ley pone sobre la Asamblea Legislativa la obligación de que las normas que prescriben las conductas prohibidas deben ser claras y precisas, de manera que se respete el principio de legalidad. En atención al tema cibernético, cabe destacar que, la tecnología se ha convertido en uno de los principales soportes del mundo que a su vez permite llevar a cabo muchas tareas en una fracción de tiempo. A medida que la computadora se ha convertido en algo común en un mundo globalizado, los crímenes han sobrepasado la esfera natural para llegar al mundo cibernético.

Se conoce como delito cibernético, cualquier conducta ilegal o delictiva en el que se haya utilizado un equipo, una *red* o un dispositivo de "hardware". Existen varios tipos de delitos cibernéticos, entre los cuales podemos mencionar: acoso cibernético, fraude, falsificación, crimen pornográfico, piratería cibernética, "Sexting", "Grooming", "Hacking", entre otros.

A continuación, traemos a colación algunos artículos periodísticos que datan y fundamentan la importancia de reglamentar este campo. *Veamos*.

Según publicado recientemente en la Red noticiosa NotiCel, las víctimas de crímenes cibernéticos en Puerto Rico perdieron en el año 2019 alrededor de $7.7 millones de dólares, de acuerdo con un informe estadístico publicado por el Negociado Federal de Investigaciones (FBI), para un total de 839 víctimas de crímenes cibernéticos en dicho año.

Por otro lado, para el 26 de enero de 2019[1], se publicó que, Puerto Rico se encuentra entre los primeros cinco mercados de mayor incidencia de ciberataques de todo el Caribe, región que es víctima de sobre 150 millones de ciberataques anuales, con pérdidas multimillonarias, sostuvo Marc Asturias, vicepresidente de Mercadeo y Relaciones Públicas de Fortinet para América Latina y el Caribe. El problema se complica ya que, según el experto, la mayoría de las víctimas, empresas como ciudadanos, desconocen que han sido "hackeados". La situación se agudiza en la medida en que se sigan ampliando "las superficies de interconexión". Se estima que cada persona cuenta hoy con entre cinco a siete dispositivos conectados a la internet, pero alrededor del 60% de las empresas que sirven a estas conexiones no poseen la capacidad de servicio de seguridad adecuada para garantizar o minimizar los ciberataques. Esta práctica a nivel global representa pérdidas ascendentes a los $7.8 trillones. Cada 39 segundos se registra un ataque y para el 2021 se estima que el daño por la ciberdelincuencia costará al mundo más de $6 billones. El 65% de todas las vulneraciones de datos involucran errores de los empleados y el 65% de los ciberataques se dirigen a las pequeñas y medianas empresas.

Asimismo, se señaló que desde el año 2011 al 2018 se había "disparado 10,000 veces lo que era antes y aunque las empresas han aumentado en un 75% sus gastos en ciber seguridad, aun no es suficiente para detener la práctica", apuntó Asturias. Sostuvo, además, que otro de los retos, es la expansión que se está experimentando a través de las cámaras de las computadoras, los monitores de los bebés, los sistemas de

[1] TECNOLOGÍA-Fuerte el reto local contra el Ciberataque, Ileanexis Vera Rosado, EL VOCERO 26/01/2019.

alarmas, entre otros servicios, que son valiosos, pero amplían la superficie de ataque, porque no están protegidos contra el "hacker".

En Puerto Rico, como en el resto del mundo, lo más frecuente es la modalidad del "fishing", que es el ataque de ingeniería social donde se recibe un correo electrónico (email), que puede ir desde ofertas de trabajo hasta maneras de ganar dinero. Mediante estos mensajes la víctima puede suplir información y automáticamente queda expuesta. Recientes investigaciones han demostrado que las impresoras son la fuente de un número creciente de amenazas a la seguridad. Actualmente una impresora tiene un 68% más de probabilidades de ser la fuente de una amenaza externa y tiene un 118% más de probabilidades de ser la fuente de una violación interna. Sin embargo, sólo el 30% de los profesionales del campo reconocen que las impresoras representan un riesgo para la seguridad.

Además, es claro que nuestro Gobierno no ha quedado inmune a los "hakers", "fishing" o la ciberdelincuencia. Como, por ejemplo, recientemente (el 13 de febrero de 2020), Puerto Rico se levantó con una noticia titulada *"Roban $1.5 millones a la Compañía de Turismo en otro caso de fraude cibernético"*. Dicha noticia relata que, la Compañía de Turismo de Puerto Rico (CTPR) sufrió un alegado fraude cibernético en diciembre de 2019 en el que fue desfalcada por $1.5 millones a una cuenta fatula, un esquema similar al que se reportó en la Compañía de Fomento Industrial (PRIDCO por sus siglas en inglés).

El director de la Unidad de Fraudes de la División de Robos a Bancos, José Ayala, confirmó a El Nuevo Día que el director de Finanzas de esa entidad recibió un correo electrónico que instruía a redirigir "pagos" a una nueva cuenta en Estados Unidos, igual que el ocurrió en el fraude denunciado por PRIDCO. De acuerdo con la investigación, el "hacker" falsificó una carta en la cual le informaba al funcionario el cambio de una cuenta bancaria de la Administración del Sistema de Retiro (ASR). Así las cosas, el funcionario procedió a emitir los pagos correspondientes a las aportaciones para el retiro o pago de pensiones sin verificar la información ni su procedencia creyendo que iban dirigidos hacia la nueva cuenta de ASR. Cuando el director de

Finanzas de Turismo se percató del esquema, procedió a radicar una querella ante las autoridades en enero de 2020.

Por otro lado, es menester señalar que, la problemática se ha incrementado ante el cierre de escuelas y oficinas para cumplir el distanciamiento social durante la Pandemia mundial COVID-19, mejor conocida como "Coronavirus". Mientras más estudiantes, padres y empleados se muevan a realizar sus labores en línea, dicho movimiento ha aumentado el riesgo de seguridad cibernética. Por ello, son sumamente necesarios los esfuerzos contemplados por el Estado para poner en vigor mecanismos de seguridad eficaces en las plataformas electrónicas utilizadas para ofrecer clases a distancia. Además, deben orientar a los padres o encargados de estudiantes sobre cómo promover dinámicas seguras mientras sus hijos participan en curso se realizan tareas en línea.

El espacio cibernético y su facilidad de acceso han dado margen al surgimiento de nuevos delitos que necesitan ser certificados como tal para poder dar justo remedio a las personas que sufren. No existe actualmente herramienta eficaz a nivel estatal que castigue las conductas indeseables de este tipo. Debemos, al igual que otros estados de los Estados Unidos de América y países del mundo, aprobar delitos que permitan llevar ante la justicia a quienes cometan tan deplorables conductas.

En la actualidad, cerca de la mitad de los jóvenes reportan ser víctimas de "cyber-bullying" y más de una tercera parte ha experimentado amenazas en línea. Las tasas más altas de suicidio, depresión y sentimientos de aislamiento son provocadas por delitos cibernéticos. Los estudios sugieren que son más propensos o expuestos los menores de 14 años, siendo estos los más vulnerables al "cyber-bullying" o a los depredadores sexuales cibernéticos. Seis de cada siete menores recibe solicitudes sexuales, usualmente de otros menores o jóvenes adultos, con quienes han compartido información personal.

Lamentablemente, existen delitos tipificados en el Código Penal y leyes especiales relacionadas a crímenes cibernéticos, de manera muy limitada. Los problemas ocasionados por los crímenes cibernéticos, por su complejidad y

características particulares, deben contar con una sección propia dentro del Código Penal, donde se recogen los delitos ordenados por tópico de esta conducta delictiva. Ello motiva la presente legislación, además de la protección de nuestra ciudadanía de este tipo de conducta indeseable.

Por tales acontecimientos, otros similares y todo lo antes expuesto es que, esta pieza legislativa representa un esfuerzo legítimo para hacer la inclusión de múltiples delitos, penas, sanciones y/o multas por conductas dentro del mundo cibernético, reformulando ciertos actos delictivos por omisión y/o negligencia en nuestro ordenamiento jurídico penal.

Este nuevo Libro Tercero ha sido atemperado a la legislación especial en este tipo de caso. Asimismo, se han redefinido e incluido nuevas figuras jurídicas para conformarlas a las directrices ofrecidas por el Tribunal Supremo de Puerto Rico y el Tribunal Supremo de Estados Unidos en interpretación de las garantías constitucionales. A esos efectos, hemos puesto énfasis sobre la protección a la intimidad, la propiedad, el patrimonio del Estado y de los individuos, los fondos públicos, la propiedad intelectual, la vida y la libertad de expresión, entre otros.

En tema del establecimiento de la responsabilidad penal, se mantiene muy presente la expresión contenida en nuestra Constitución que establece con jerarquía constitucional el carácter rehabilitador de la pena al disponer en su Artículo VI, Sección 19, que las instituciones penales preponderarán "el tratamiento adecuado de los delincuentes para hacer posible su rehabilitación moral y social"; que "no se impondrán castigos crueles e inusitados" y que las "multas no serán excesivas". Artículo II, Secciones 11 y 12 de la Constitución del Estado Libre Asociado de Puerto Rico. A esos efectos, se reconocen como principios fundamentales que la sanción penal no podrá atentar contra la dignidad humana y la rehabilitación moral y social del convicto como un objetivo general para la imposición de las penas. De igual manera, ponemos especial atención en velar por la confianza pública imponiendo sobre los funcionarios o empleados públicos la obligación de rectitud e integridad en el cumplimiento de su

deber y la destitución de su cargo o empleo como pena cuando infrinja la ley en el desempeño de las funciones públicas.

DECRÉTASE POR LA ASAMBLEA LEGISLATIVA DE PUERTO RICO:

Sección 1.- Se añade un nuevo Libro Tercero – Ciberdelincuencia a la Ley Núm. 146-2012, según enmendada, conocida como el "Código Penal de Puerto Rico", para que lea como sigue:

"LIBRO TERCERO – PARTE ESPECIAL: CIBERDELINCUENCIA

TÍTULO I – ACCESO INDEBIDO A SISTEMAS INFORMÁTICOS

CAPÍTULO I – DELITOS INFORMÁTICOS COMO OBJETO

SECCIÓN PRIMERA – DEFINICIONES

Artículo 301.- Definiciones.

1) *Acceso Ilícito o Piratería, se entiende como cualquier medio para entrar a otro sistema informático, con inclusión de los ataques por internet, así como el acceso ilícito a las redes inalámbricas y el acceso no autorizado a los ordenadores que no están conectados a ninguna red.*
2) *Acceso Ilegal o Indebido a los Sistemas de Información, se entiende como el acceso no autorizado, al conjunto o a una parte de un sistema de información cuando se comete transgrediendo medidas de seguridad.*
3) *Adquisición Ilegal, se entiende como la interceptación de los procesos de transferencia de datos.*
4) *Ataques a la Integridad del Sistema, se entiende como toda obstaculización deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.*

5) *Datos Informáticos, se entiende toda representación de hechos, información o conceptos de una forma que permita su procesamiento en un sistema de computadoras, incluido un programa capaz de provocar que un sistema informático realice una función.*

6) *Difusión de Material Racista y Xenófobo Mediante Sistemas Informáticos, se entiende como todo material escrito, toda imagen o cualquier otra representación de ideas o teorías, que propugne, promueva o incite al odio, la discriminación o la violencia, contra cualquier persona o grupo de personas, por razón de raza, color, ascendencia u origen nacional o étnico, así como de la religión.*

7) *Espionaje de Datos, se entiende como toda persona que, intencionalmente, sin excusa o justificación legal o en exceso de una excusa o justificación legal obtenga, para sí o para otro, datos informáticos que no estén destinados a él y que estén especialmente protegidos contra el acceso no autorizado.*

8) *Espionaje Económico, se entiende como toda persona que, intencionalmente o a sabiendas de que la intrusión beneficiará a cualesquiera gobiernos, agencias o agentes extranjeros:*

   a) *robe o, sin autorización, se apropie de, tome, se lleve u oculte, o mediante fraude, artificio o engaño, obtenga un secreto comercial;*

   b) *sin autorización copie, duplique, esboce, dibuje, fotografíe, descargue, cargue, altere, destruya, fotocopie, replique, transmita, entregue, expida, envíe por correo electrónico, comunique o transporte un secreto comercial;*

c) reciba, compre o posea un secreto comercial, a sabiendas de que éste ha sido robado o ha sido objeto de apropiación, obtenido o convertido sin autorización;

d) intente cometer cualesquiera de los actos descritos en los anteriores incisos a) b) y c); o

e) conspire con una o más personas para cometer cualquiera de los actos descritos en los anteriores incisos a) b) y c) y una o más de esas personas actúe para llevar a la práctica el objeto de la conspiración.

9) Falsificación Informática o "Phishing", se entiende como la introducción, alteración, borrado o supresión deliberados e ilegítimos de datos informáticos que genere datos no auténticos con la intención de que sean tomados o utilizados a efectos legales como auténticos, con la independencia de que los datos sean legibles e inteligibles directamente.

10) Hostigamiento, Intimidación o "Cyberbullying", se entiende como cualquier patrón de acciones realizados intencionalmente, ya sea mediante abuso psicológico, físico, cibernético o social, que tenga el efecto de atemorizar a una persona o a un grupo de personas.

11) Incautar, incluye:

a) activar cualquier computadora y medio de almacenamiento de datos informáticos;

b) crear y conservar una copia de datos informáticos;

c) mantener la integridad de los datos informáticos pertinentes almacenados;

d) suprimir o hacer que no pueda accederse a datos informáticos existentes en el sistema de computadoras al que se accede;

e) imprimir una copia de los datos informáticos salientes; o

f) incautar o asegurar de manera similar un sistema de computadoras o parte del mismo, o un medio de almacenamiento de datos informáticos.

12) Infraestructura Esencial, se entiende como aquellos sistemas, aparatos y redes de información, programas y datos informáticos que resultan tan vitales para el país que la incapacitación, destrucción o interferencia de tales sistemas y activos supondría un menoscabo de la seguridad, la seguridad económica o nacional, la salud y protección pública general o cualquier combinación de estos factores.

13) Interceptación, se entiende, entre otras cosas, la adquisición, visualización y captación de cualquier comunicación de datos informáticos, ya sea por medios alámbricos, inalámbricos, electrónicos, ópticos, magnéticos, verbales o de otro tipo, durante la transmisión a través de la utilización de cualquier dispositivo técnico.

14) Interferencia con Datos, se entiende como toda persona que, deliberada o imprudentemente, sin excusa o justificación legal, realice cualesquiera de los siguientes actos:

a) destruya o altere datos; o

b) haga que los datos resulten incompresibles, inútiles o ineficaces; o

c) obstruya, interrumpa o interfiera con la utilización legal de los datos; o

d) obstruya, interrumpa o interfiera con cualquier persona en la utilización legal de los datos; o

e) deniegue el acceso a los datos a cualquier persona con derecho a acceder a los mismos.

El inciso a) se aplica independientemente del hecho de que el acto de la persona tenga un efecto temporal o permanente.

15) *Interceptación Ilegal, se entiende como la obtención o intrusión deliberada e ilegítima por medios técnicos de datos informáticos en transmisiones no publicas dirigidas a un sistema informático, originados en un sistema informático o efectuados dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos.*

16) *Material Erótico, Obsceno y Pornográfico, comprende de cualquier libro, revista, periódico u otro material impreso, escrito, o digital, o cualquier retrato, fotografía, dibujo, caricatura, película de movimiento, cinta cinematográfica u otra representación gráfica; o cualquier representación oral o visual transmitida o retransmitida a través de cables, ondas electromagnéticas, computadoras, tecnología digital o cualesquiera medios electrónicos o de comunicación telemática; o cualquier estatua, talla o figura, escultura; o cualquier grabación, transcripción o reproducción mecánica, química o eléctrica o cualquier otro artículo, equipo o máquina.*

Además, se entiende como "material" todo aquello que considerado en su totalidad por una persona promedio y que al aplicar patrones comunitarios contemporáneos:

a) apele al interés lascivo, o sea, a un interés morboso en la desnudez, sexualidad o funciones fisiológicas;

b) represente o describa en una forma patentemente ofensiva conducta sexual; y

c) carezca de un serio valor literario, artístico, religioso, científico o educativo.

La atracción del material al interés lascivo en el sexo se juzga en referencia al adulto promedio, a menos que se desprenda de la naturaleza del material, o de las circunstancias de su diseminación, distribución o exhibición, que está diseñado para grupos de desviados sexuales, en cuyo caso dicha atracción se juzgará con referencia al grupo a quien va dirigido.

En procesos de violación a las disposiciones de esta Sección, donde las circunstancias de producción, presentación, venta, diseminación, distribución, o publicidad indican que el acusado está explotando comercialmente el material por su atracción lasciva, la prueba de este hecho constituirá prueba prima facie de que el mismo carece de serio valor literario, artístico, religioso, científico o educativo.

Cuando la conducta prohibida se lleve a cabo para o en presencia de menores será suficiente que el material esté dirigido a despertar un interés lascivo en el sexo.

Cualquier tipo de anuncio o facilitación de actividad sexual por internet.

17) Medio de Almacenamiento de Datos Informáticos, se entiende como todo artículo o material a partir del cual es posible reproducir información, con o sin ayuda de cualquier otro artículo o dispositivo.

18) Permanencia Ilegal, se entiende como toda persona que intencionalmente, sin autorización o justificación legal, o excediéndose de una excusa o justificación legal, permanezca conectado en un sistema informático o en parte de un sistema informático o siga utilizando un sistema informático.

19) Perturbación, se entiende como manipulaciones que comprenden:

a) cortar el suministro eléctrico a un sistema de computadoras;

b) causar interferencias electromagnéticas a un sistema de computadoras;

c) corromper por cualquier medio un sistema de computadoras; e

d) ingresar, transmitir, dañar, borrar, deteriorar, alterar o suprimir datos informáticos del sistema.

20) Pornografía Infantil, se entiende como toda representación, por cualquier medio, de un menor de edad o persona que luzca como tal, dedicado a actividades sexuales explicitas o implícitas, reales o simuladas, o toda representación de las partes genitales de un menor de edad o persona que luzca como tal, con fines primordialmente sexuales. Esta incluye, pero no se limita a, todo material pornográfico sonoro, visual o escrito.

21) Programas Maliciosos o "Malware", se entiende como aquella programación creada para causar daño a un dispositivo, sistemas o a sus usuarios, que pueden incluir desde danos leves hasta destrucción total del sistema.

22) Protocolo de Internet o "IP", se entiende como las direcciones numéricas estándar que se emplea para el envío y recepción de información mediante una red con la posibilidad de confirmar que un paquete de información o datos llegó a su destino.

23) Proveedor de Hospedaje, se entiende como toda persona física o jurídica que presta un servicio de transmisión electrónica de datos mediante el almacenamiento de la información proporcionada por un usuario del servicio.

24) Proveedor de Servicio, se entiende como toda entidad pública o privada que ofrece a los usuarios de su servicio la capacidad de comunicar por medio de un sistema de

computadoras, y cualquier otra entidad que procese o almacene datos informáticos en nombre de dicho servicio de comunicación o de los usuarios de dicho servicio.

25) Redes Informáticas, se entiende como un grupo de sistemas interconectados o relacionados en que uno o varios de ellos llevan a cabo, con arreglo a un programa, el procesamiento automático de datos o cualquier otra función análoga.

26) Seducción de un Menor de Edad, Preparación o Captación, o "Grooming", se entiende como aquel acto preparatorio mediante las tecnologías de la información y la comunicación, con el fin de proponer un encuentro con un menor de edad con el fin de abusar sexualmente de él.

27) Sistema Informático, se entiende como un aparato o grupo de aparatos interconectados o relacionados, en que uno o varios de ellos lleva a cabo, con arreglo a un programa, el procesamiento automático de datos o cualquier otra función.

28) Usurpación de Identidad, se entiende como el acto de obtener, poseer, transferir o utilizar información relacionada con la identidad de otra persona, sin autorización para ello.

SECCIÓN SEGUNDA – DELITOS INFORMÁTICOS Y CONEXOS

Artículo 302.- Acceso Indebido a Sistema Informático.

El que, sin autorización o excediendo una autorización en todo o en parte acceda a un sistema informático o sistema telemático o de telecomunicaciones, o a sus componentes, 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 exigirlo, incurrirá en delito menos grave.

Cuando de dicho acceso ilícito resulte la supresión o la modificación de datos, información o contenido en el sistema, o revelen o difundan datos confidenciales o personales contenidos en el sistema accesado, será sancionada con pena de reclusión por un término fijo de cinco (5) años.

Artículo 303.- Sabotaje Informático.

Toda persona que, sin autorización o excediendo una autorización, destruya o inutilice en todo o en parte un sistema informático o sistema telemático o de telecomunicaciones o a sus componentes, o impida, altere, entorpezca, obstaculice o modifique su funcionamiento o uso regular o acceso, protegido o no con una medida de seguridad, será sancionada con pena de reclusión por un término fijo de tres (3) años.

Artículo 304.- Sabotaje Informático Agravado.

Será sancionada con pena de reclusión por un término fijo de cinco (5) años toda persona que cometa el delito de sabotaje informático descrito en el Articulo 303, cuando se lleve a cabo para beneficio personal o de un tercero. El tercero beneficiado también incurrirá en este delito.

Si la persona obtiene o logra el beneficio personal perseguido, será sancionada con pena de reclusión por un término fijo de ocho (8) años.

Artículo 305.- Ataque a la Integridad de Sistemas Informáticos del Sistema Público.

Toda persona que, sin autorización o excediendo una autorización, destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprema datos informáticos, mensajes de correo electrónicos, a sistemas del servicio público del Gobierno de Puerto Rico, cuyo contenido sea esencial para su

funcionamiento o desarrollo de programas, de tratamiento de información, telemático o de telecomunicaciones a todo o en parte de sus componentes, protegido o no con una medida de seguridad, será sancionada con pena de reclusión por un término fijo de ocho (8) años.

Artículo 306.- Ataque a la Integridad de Sistemas Informáticos del Sistema Público Agravado.

Sera sancionada con pena de reclusión por un término fijo de diez (10) años toda persona que cometa el delito de ataque a la integridad de sistemas informáticos del sistema público descrito en el Articulo 305, cuando de dicho acceso ilícito sobrevenga peligro colectivo o daño social.

Si del delito descrito en el párrafo anterior sobreviene la pérdida de fondos públicos que sobrepase de cinco (5,000) mil dólares, será sancionada con pena de reclusión por un término fijo de quince (15) años. El Tribunal también podrá imponer pena de restitución.

Artículo 307.- Explotación Informática.

El que, sin autorización o excediendo una autorización en todo o en parte accese a un sistema informático o sistema telemático o de telecomunicaciones 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 exigirlo, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar el tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pago a los proveedores legítimos de los servicios, será sancionada con pena de reclusión por un término fijo de ocho (8) años.

Artículo 308.- Daño Informático.

Toda persona que, sin autorización o excediendo una autorización a propósito, con conocimiento o temerariamente, destruya, dañe o vandalice en todo o en parte los datos contenidos en un sistema de información, telemático o de telecomunicaciones o de sus componentes, protegido o no con una medida de seguridad, o en perjuicio de un tercero, suprima, modifique o destruya la información contenida, será sancionada con pena de reclusión por un término fijo de cinco (5) años.

La persona que resulte convicta por el delito descrito en el párrafo anterior será sancionada con pena de reclusión por un término fijo de tres (3) años cuando la comisión del delito se cometiere por negligencia, imprudencia, impericia o inobservancia.

Artículo 309.- Daño Informático Agravado.

Sera sancionada con pena de reclusión por un término fijo de ocho (8) años toda persona que cometa el delito de daño informático descrito en el Articulo 308, cuando se cometiere en contra de los componentes de un sistema informático que utilice tecnologías de información y comunicación, destinadas a la prestación de servicios públicos o financieros, o que contengan información personal, confidencial, reservada, patrimonial, técnica o propia de personas naturales o jurídicas.

Artículo 310.- Revelación de Secretos.

Toda persona que, sin autorización o excediendo una autorización a propósito, con conocimiento o temerariamente modifique, destruya, obtenga, copie o utilice información de seguridad publica en todo o en parte de los datos contenidos en un sistema de información, telemático o de telecomunicaciones o de sus componentes, protegido o no con

una medida de seguridad, será sancionada con pena de reclusión por un término fijo de cinco (5) años.

Artículo 311.- Revelación de Secretos Agravado.

Sera sancionada con pena de reclusión por un término fijo de ocho (8) años toda persona que para beneficio personal o de un tercero, cometa el delito de revelación de secretos descrito en el Articulo 310, cuando la conducta obstruya, entorpezca, obstaculice, limite o imposibilite la administración o aplicación de la justicia, o recaiga sobre los registros relacionados con un procedimiento penal resguardados por las autoridades competentes. El tercero beneficiado también incurrirá en este delito.

Cuando el autor del delito descrito en el párrafo anterior se cometiere por un funcionario público, será sancionada con pena de reclusión por un término fijo de quince (15) años. Además, se impondrá destitución e inhabilitación de cuatro (4) a diez (10) años para desempeñarse en otro empleo, puesto o cargo público.

Artículo 312.- Instalación o Propagación de Programas Informáticos Maliciosos.

Toda persona que, sin autorización o excediendo una autorización a propósito y por cualquier medio, instale programas informáticos maliciosos en un sistema o red informática o telemática, o en los contenedores electrónicos, ópticos o magnéticos, o de sus componentes, protegido o no con una medida de seguridad, será sancionada con pena de reclusión por un término fijo de tres (3) años.

Artículo 313.- Instalación o Propagación de Programas Informáticos Maliciosos Agravado.

Sera sancionada con pena de reclusión por un término fijo de cinco (5) años toda persona que cometa el delito de instalación o propagación de programas informáticos descrito en el Articulo 312, cuando se induzca a error a otra persona para que instale un programa malicioso en un sistema o red informática o telemática, o en los contenedores electrónicos, ópticos o magnéticos, sin la debida autorización; 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; 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; quien distribuya programas informáticos diseñados para la creación de programas informáticos maliciosos; quien ofrezca, contrate o brinde servicios de denegación de servicios, envío de comunicaciones masivas no solicitadas, o propagación de programas informáticos maliciosos, para beneficio personal o de un tercero.

Cuando el autor del delito descrito en el párrafo anterior, afecte a una entidad bancaria, financiera, cooperativa de ahorro y crédito, asociación solidarista o ente estatal; afecte el funcionamiento de servicios públicos; obtenga el control a distancia de un sistema o de una red informática para formar parte de otra red de ordenadores; esté diseñado para realizar acciones dirigidas a procurar un beneficio patrimonial para sí o para un tercero; afecte sistemas informáticos de la salud y la afectación de estos pueda poner en peligro la salud o vida de las personas; o tenga la capacidad de reproducirse sin la necesidad de intervención adicional por parte del usuario legítimo del sistema

informático, será sancionada con un pena de reclusión por un término fijo de ocho (8) años.

Artículo 314.- Uso de Programas Destructivos.

Toda persona que, con la intención de producir un daño, adquiera, distribuya o ponga en circulación programas o instrucciones informáticas destructivas, que puedan causar perjuicio a los registros, programas o a los equipos de computación, será sancionada con pena de reclusión por un término fijo de un (1) año.

Artículo 315.- Dispositivos Fraudulentos.

Toda persona que, produzca, use, posea, trafique o distribuya, sin autoridad o causa legitima, programas informáticos, equipos, materiales o dispositivos cuyo único uso o uso fundamental sea el de emplearse como herramienta para cometer crímenes y delitos de alta tecnología, será sancionada con pena de reclusión por un término fijo de ocho (8) años.

Artículo 316.- Suplantación de Páginas Electrónicas.

Toda persona que, con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o suplante páginas electrónicas, enlaces o ventanas emergentes, será sancionada con pena de reclusión por un término fijo de tres (3) años.

Artículo 317.- Suplantación de Páginas Electrónicas Agravado.

Será sancionada con pena de reclusión por un término fijo de ocho (8) años toda persona que para beneficio personal o de un tercero, cometa el delito de suplantación de páginas electrónicas descrito en el Articulo 316, cuando la conducta 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.

Artículo 318.- Facilitación del Delito.

Toda persona que, 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, será sancionada con pena de reclusión por un término fijo de cinco (5) años.

Artículo 319.- Facilitación del Delito Agravado.

Será sancionada con pena de reclusión por un término fijo de ocho (8) años toda persona que, cometa el delito de facilitación del delito descrito en el Articulo 318, cuando la información obtenida se utilice en provecho propio o ajeno.

Artículo 320.- Utilización Ilícita de Redes de Comunicaciones.

Toda persona que, con fines ilícitos haga uso de aparatos de radiofonía o televisión, o de cualquier medio electrónico diseñado o adaptado para interferir, emitir o reproducir señales, sin autorización, será sancionada con pena de reclusión por un término fijo de tres (3) años.

Artículo 321.- Manipulación de Equipos o Terminales Móviles.

Toda persona que, manipule, reprograme, remarque o modifique los terminales móviles de los servicios de comunicaciones en cualquiera de sus componentes, con el fin de alterar las bases de datos positivas y negativas que se crearán para el efecto y que

administrará la entidad regulatoria correspondiente, será sancionada con pena de reclusión por un término fijo de cuatro (4) años.

Artículo 322.- Manipulación de Equipos o Terminales Móviles Agravado.

Será sancionada con pena de reclusión por un término fijo de ocho (8) años toda persona que, cometa el delito de manipulación de equipos o terminales móviles descrito en el Articulo 321, cuando las conductas resulten ser parte de una red, grupo u organización de carácter delincuencial o criminal.

Artículo 323.- Manipulación de Equipos de Localización y Vigilancia.

Toda persona que, retire, modifique o inutilice, sin la debida autorización, dispositivos de localización y vigilancia, será sancionada con pena de reclusión por un término fijo de cinco (5) años.

Artículo 324.- Manipulación de Equipos de Localización y Vigilancia Agravado.

Será sancionada con pena de reclusión por un término fijo de diez (10) años toda persona que, cometa el delito de manipulación de equipos de localización y vigilancia descrito en el Articulo 323, cuando se cometiere por un funcionario público. Además, se impondrá destitución e inhabilitación de cuatro (4) a diez (10) años para desempeñarse en otro empleo, puesto o cargo público.

Artículo 325.- Intercambio, Comercialización o Compra de Información de Equipos o Terminales Móviles.

Toda persona que, intercambie, comercialice o compre bases de datos que contengan información de identificación de equipos terminales móviles, será sancionada con pena de reclusión por un término fijo de tres (3) años.

CAPÍTULO II – DELITOS INFORMÁTICOS COMO MEDIO

SECCIÓN PRIMERA – DELITOS SEXUALES

Artículo 326.- Corrupción.

Toda persona que, procure su excitación sexual o la excitación sexual de otro, realizare acciones de significación sexual ante un menor de edad, le hiciere ver o escuchar material pornográfico o presentar espectáculos del mismo carácter, por medio de las tecnologías de información y la comunicación, será sancionada con pena de reclusión por un término fijo de cinco (5) años.

Artículo 327.- Corrupción Agravado.

Será sancionada con pena de reclusión por un término fijo de diez (10) años toda persona que, cometa el delito de corrupción descrito en el Articulo 326, cuando con el fin de procurar su excitación sexual o la excitación sexual de otro, obligue, induzca, persuada, sugiera, incite, o convenza a una persona menor de edad a realizar acciones de significación sexual delante suyo o de otro; o a enviar, entregar o exhibir imágenes o grabaciones de su persona a otro menor de edad aunque haya expresado su consentimiento.

Será sancionada con pena de reclusión por un término fijo de quince (15) años, todo aquel que procure, promueva, obligue, publicite, gestione, facilite o induzca, por cualquier medio, a una persona menor de dieciocho años de edad, o que no tenga la capacidad de comprender el significado del hecho, o no tenga capacidad de resistir la conducta, a realizar actos sexuales o de exhibicionismo corporal, con fines sexuales, reales o simulados, con el objeto de producir material a través de video grabarlas, audio

grabarlas, fotografiarlas, filmarlos, exhibirlos o describirlos a través de anuncios impresos, sistemas de cómputo, electrónicos o sucedáneos, y se beneficie económicamente de la explotación de la persona.

Si se hiciere el uso de la fuerza, el engaño, la violencia física o psicológica, la coerción, el abuso de poder o de una situación de vulnerabilidad, las adicciones, una posición jerárquica o de confianza, o la concesión o recepción de pagos o beneficios para obtener el consentimiento de una persona que tenga autoridad sobre otra o cualquier otra circunstancia que disminuya o elimine la voluntad de la víctima para resistirse, la pena prevista en el párrafo anterior se aumentará en una mitad.

Artículo 328.- Explotación Sexual, Pornografía y Acto Sexual con Menores de Edad.

Toda persona que, con ánimo de lucro, beneficio personal o para un tercero, induzca facilite, promueva o utilice, con fines sexuales o eróticos a una persona menor de edad o con discapacidad haciéndola presenciar o participar en un comportamiento sexual, espectáculo público o privado, aunque la victima consienta presenciar tal comportamiento o participar en él, por medio de las tecnologías de información y la comunicación, será sancionada con pena de reclusión por un término fijo de diez (10) años.

Artículo 329.- Fabricación, Producción, Difusión o Reproducción de Pornografía.

Toda persona que participare en la producción, financiación, fabricación, reproducción, publicación, comercialización, importe, exporte, difusión, o en la distribución de material pornográfico, por cualquier medio, sea directo, mecánico, digital, audio, visual o con soporte informático, electrónico u otros conexos, en cuya elaboración hubieren sido utilizados menores de edad, será sancionada con pena de reclusión por un

término fijo de diez (10) años. Se entenderá por material pornográfico en cuya elaboración hubieren sido utilizados menores de edad, toda representación de éstos dedicados a actividades eróticas o sexuales explícitas o implícitas, reales o simuladas, o toda representación de sus partes genitales con fines sexuales, o toda representación de dichos menores en que se emplee su voz o imagen, con los mismos fines.

Artículo 330.- Pornografía Relativa a Menores de Edad.

Toda persona que fotografíe, filme, grabe, produzca, divulgue, ofrezca, venda, compre, posea, porte, almacene, trasmita o exhiba, por cualquier medio, para uso personal o intercambio, representaciones reales de actividad sexual que involucre una persona menor de edad, será sancionada con pena de reclusión por un término fijo de diez (10) años.

Artículo 331.- Pornografía Relativa a Menores de Edad Agravado.

Será sancionada con pena de reclusión por un término fijo de quince (15) años toda persona que, cometa el delito de pornografía relativa a menores de edad descrito en el Articulo 330, quien alimente con pornografía infantil bases de datos de Internet, con o sin fines de lucro.

La pena se aumentará de una tercera parte a la mitad cuando el responsable sea integrante de la familia de la víctima, dentro del cuarto grado de consanguinidad o segundo de afinidad.

Artículo 332.- Pornografía Virtual y Pseudo Pornografía.

Toda persona que posea, produzca, venda, distribuya, exhiba o facilite, por cualquier medio, material pornográfico en el que no habiendo utilizado personas menores

de edad, emplee a una persona adulta que simule ser una persona menor de edad realizando actividades sexuales; o emplee imagen, caricatura, dibujo o representación, de cualquier clase, que aparente o simule a una persona menor de edad realizando actividades sexuales, será sancionada con pena de reclusión por un término fijo de quince (15) años.

Artículo 333.- Tenencia, Adquisición o Posesión de Material Pornográficos de Menores de Edad o Personas con Impedimentos.

Toda persona 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 un menor de edad o persona con discapacidad o su imagen para su producción, será sancionada con pena de reclusión por un término fijo de diez (10) años.

Artículo 334.- Difusión de Pornografía.

Toda persona quien entregue, comercie, difunda, distribuya o exhiba material pornográfico de personas menores de edad o incapaces, 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 un menor de edad o persona con discapacidad o su imagen para su producción, será sancionada con pena de reclusión por un término fijo de diez (10) años.

El que maliciosamente adquiera o almacene material pornográfico, cualquiera sea su soporte, en cuya elaboración hayan sido utilizados menores de edad, será sancionada con pena de reclusión por un término fijo de tres (3) años.

Artículo 335.- Utilización o Facilitación de Medios de Comunicación para Actividades Sexuales con Menores de Edad o Personas con Impedimentos.

Toda persona que, de cualquier modo, facilitare, en beneficio propio o ajeno, la comercialización, difusión, exhibición, importación, exportación, distribución, oferta, almacenamiento o adquisición de material pornográfico que contenga la imagen o cualquier otra forma de representación de una o más personas menores de edad o incapaces, será sancionada con pena de reclusión por un término fijo de cinco (5) años.

Artículo 336.- Comercialización de Pornografía con Menores de Edad o Personas con Impedimentos.

Toda persona que, publique, compre, posea, porte, transmita, descargue, almacene, importe, exporte o venda, por cualquier medio, para uso personal o para intercambio pornografía de menores de edad, será sancionada con pena de reclusión por un término fijo de diez (10) años.

Artículo 337.- Exhibición Pornográfica.

Toda persona que, ofrezca o publique espectáculos teatrales o cinematográficos obscenos, transmita audiciones o efectúe publicaciones de idéntico carácter, será sancionado con pena de reclusión por un término fijo de diez (10) años.

Artículo 338.- Turismo Sexual.

Toda persona que, promueva, publique, invite, facilite o gestione por cualquier medio a que una o más personas viajen al interior o exterior del territorio y jurisdicción de Puerto Rico con la finalidad de que realice cualquier tipo de actos sexuales reales o simulados con una o varias personas menores de edad, o con una o varias personas que no

tienen capacidad para comprender el significado del hecho o con una o varias personas que no tienen capacidad para resistirlo, será sancionada con pena de reclusión por un término fijo de quince (15) años.

Artículo 339.- Destrucción de Material.

Cuando medie convicción y sentencia firme por cualquier delito comprendido en esta Sección, el tribunal ordenará que se destruya cualquier material o anuncio obsceno o de pornografía infantil que haya motivado la convicción del acusado y que se encuentre en poder o bajo control del tribunal, del ministerio público o de un funcionario del orden público.

SECCIÓN SEGUNDA – DELITOS CONTRA LA INTIMIDAD

Artículo 340.- Acceso Indebido a Datos.

Toda persona que, sin autorización y violando sistemas de seguridad obtuviere para sí o para terceros, el acceso a datos no destinados a él y especialmente protegidos contra el acceso no autorizado, será sancionada con pena de reclusión por un término fijo de tres (3) años.

Artículo 341.- Acceso Indebido a Datos del Sistema Público y del Gobierno de Puerto Rico.

Será sancionada con pena de reclusión por un término fijo de cinco (5) años toda persona que, cometa el delito de acceso indebido a datos descrito en el Articulo 340, cuando se cometiere por un funcionario público. Además, se impondrá destitución e inhabilitación de cuatro (4) a diez (10) años para desempeñarse en otro empleo, puesto o cargo público, o según se establezca en leyes especiales aplicables.

Artículo 342.- Uso de Equipos para Invasión de Privacidad.

Toda persona que, use, sin causa legítima o autorización de la entidad legalmente competente, de sistemas electrónicos, informáticos, telemáticos, de telecomunicaciones, o dispositivos que puedan servir para realizar operaciones que atenten contra la privacidad en cualquiera de sus formas, será sancionada con pena de reclusión por un término fijo de dos (2) años.

Artículo 343.- Acceso Indebido a Correspondencia o Comunicaciones del Sistema Público y del Gobierno de Puerto Rico.

Toda persona será sancionada con pena de reclusión por un término fijo de cinco (5) años, cuando:

(a) opere o abuse de los servicios o instalaciones de telecomunicaciones de libre recepción o de radiodifusión sin autorización de la autoridad correspondiente, y el que permita que, en su domicilio, residencia, morada o medio de transporte, operen tales servicios o instalaciones; o

(b) maliciosamente interfiera, intercepte o interrumpa un servicio de telecomunicaciones, y la confiscación de los equipos e instalaciones; o

(c) intercepte o capte maliciosamente o grave sin la debida autorización, cualquier tipo de señal que se emita a través de un servicio público de telecomunicaciones; o

(d) difusión pública o privada de cualquier comunicación obtenida por infracción(es) a las disposiciones bajo este Artículo.

Artículo 344.- Acceso Indebido a Correspondencia o Comunicaciones del Sistema Público y del Gobierno de Puerto Rico Agravado.

Será sancionada con pena de reclusión por un término fijo de diez (10) años toda persona que, cometiere el delito de acceso indebido a correspondencia o comunicaciones del sistema público y del gobierno de Puerto Rico descrito en el Articulo 343, cuando se cometiere por un funcionario público, o persona encargada de la recolección, entrega o salvaguarda de los documentos o comunicaciones, o persona encargada 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.

Además, si la convicción resulta por un funcionario público, se impondrá destitución e inhabilitación de cuatro (4) a diez (10) años para desempeñarse en otro empleo, puesto o cargo público, o según se establezca en leyes especiales aplicables.

Artículo 345.- Acceso Indebido o Ilícito de Información Médica.

Toda persona que, sin autorización, violando o no los sistemas de seguridad, obtuviere para sí o para terceros, el acceso a datos médicos de otra persona, no destinados a él y especialmente protegidos contra el acceso no autorizado, será sancionada con pena de reclusión por un término fijo de cinco (5) años.

Será sancionada con pena de reclusión por un término fijo de siete (7) años toda persona que, cometa el delito de acceso indebido o ilícitos de información médica, cuando se cometiere por un funcionario público. Además, se impondrá destitución e inhabilitación de cuatro (4) a diez (10) años para desempeñarse en otro empleo, puesto o cargo público.

Artículo 346.- Acceso Indebido o Ilícito de Información Médica Agravado.

Será sancionada con pena de reclusión por un término fijo de diez (10) años toda persona que, cometiere el delito de acceso indebido o ilícito de información médica descrito en el Artículo 345, cuando con peligro o daño para la intimidad de otro, utilice o difunda el contenido de comunicaciones o documentos privados que carezcan de interés público.

Artículo 347.- Interceptación de Datos Informáticos.

Toda persona 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, será sancionada con pena de reclusión por un término fijo de tres (3) años, cuando:

(a) 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; o

(b) 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; o

(c) 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; o

(d) produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior.

Artículo 348.- Obtención y Transferencia de Información Confidencial.

Toda persona que, deliberadamente obtenga y transfiera información de carácter confidencial y que mediante el uso de esa información vulnere un sistema o datos informáticos apoyándose en cualquier clase de las tecnologías de la información y la comunicación, incluidas las emisiones electromagnéticas, será sancionada con pena de reclusión por un término fijo de cinco (5) años.

Artículo 349.- Obtención y Transferencia de Información Confidencial del Sistema Público o del Gobierno de Puerto Rico.

Será sancionada con pena de reclusión por un término fijo de siete (7) años toda persona que, cometa el delito de acceso indebido a correspondencia o comunicaciones del sistema público y del gobierno de Puerto Rico descrito en el Articulo 348, cuando se cometiere por un funcionario público. Además, se impondrá destitución e inhabilitación de cuatro (4) a diez (10) años para desempeñarse en otro empleo, puesto o cargo público.

Artículo 350.- Apertura o Interceptación Ilegal de Comunicaciones.

Toda persona que ilegítimamente abra, intercepte, o por cualquier otro medio se entere del contenido de un documento, un pliego cerrado o un despacho telegráfico,

telemático, electrónico o de otra naturaleza que no le esté dirigido, será sancionada con pena de reclusión por un término fijo de un (1) año.

Artículo 351.- Violación a la Intimidad.

Toda persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena de reclusión por un término fijo de tres (3) años.

Artículo 352.- Revelación Indebida de Datos e Información.

Será sancionada con pena de reclusión por un término fijo de diez (10) años toda persona que, cometiere el delito de extorsión informática "ransomware" descrito en el Artículo 363, cuando se hubiese realizado con ánimo de lucro, la comisión de otro delito o se difunda material sexual explícito en perjuicio de un tercero.

Artículo 353.- Preparación de Acceso Indebido o Intercepción de Datos.

Toda persona que, prepare un hecho punible según los Artículos 340, 341, 342, 343, 344, 345, 346, 347, 348, 349, 350, 351 y 352 produciendo, difundiendo o haciendo accesible de otra manera a terceros:

(a) las claves de acceso u otros códigos de seguridad, que permitan el acceso a datos; o

(b) los programas de computación destinados a la realización de tal hecho.

Será sancionada con pena de reclusión por un término fijo de tres (3) años.

SECCIÓN TERCERA – DELITOS CONTRA LA IDENTIDAD

Artículo 354.- Hurto, Supresión, Alteración de Identidad o de Estado Civil.

Toda persona que, ilegalmente impida, altere, añada o suprima la inscripción de los datos de identidad suyos o inscriba como suya o de otra persona en programas informáticos, partidas, tarjetas de identificación "Real ID", licencia de conducir o en cualquier otro documento emitido por el Gobierno de Puerto Rico, será sancionada con pena de reclusión por un término fijo de cinco (5) años.

Además, toda persona que, ilegalmente altere la identidad de un(a) menor de edad; la sustituya por otra; entregue o consigne datos falsos o supuestos sobre un nacimiento; usurpe la legítima paternidad o maternidad de un(a) menor de edad o declare falsamente el fallecimiento de un recién nacido, será sancionada con pena de reclusión por un término fijo de siete (7) años.

SECCIÓN CUARTA – DELITOS CONTRA LA PERSONA

Artículo 355.- Revelación y Transmisión Ilegal de Base de Datos.

Toda persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena de reclusión por un término fijo de tres (3) años.

Artículo 356.- Revelación y Transmisión Ilegal de Base de Datos Agravado.

Será sancionada con pena de reclusión por un término fijo de cinco (5) años toda persona que, cometa el delito de revelación y transmisión ilegal de base de datos descrito

en el Articulo 358, cuando se cometiere por un funcionario público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas. Además, se impondrá destitución e inhabilitación de cuatro (4) a diez (10) años para desempeñarse en otro empleo, puesto o cargo público.

Artículo 357.- Publicidad o Comercio de Personas, Órganos, Servicios o Bienes Ilícitos.

Toda persona que, por cualquier medio que involucre el uso de las tecnologías de la información y la comunicación, promueva, favorezca, facilite o publique la oferta, la obtención o el tráfico ilegal de órganos y tejidos humanos o el trasplante de los mismos, o se beneficie económicamente de la explotación de una persona mediante el comercio, distribución, exposición, circularización u oferta de libros, revistas, escritos, grabaciones, filmes, fotografías, anuncios impresos, imágenes u objetos, de carácter lascivo o sexual, reales, o simulados, sea de manera física, o a través de cualquier medio, será sancionada con pena de reclusión por un término fijo de quince (15) años.

Artículo 358.- Propalación o "Pornovenganza".

Toda persona quien, hallándose legítimamente en posesión de una comunicación, de documentos o grabaciones de carácter privado, los haga públicos sin la debida autorización, aunque le hayan sido dirigidos, será sancionada con pena de reclusión por un término fijo de tres (3) años.

Además, cuando se trate de documentos divulgados por internet, o las grabaciones, imágenes, comunicaciones o documentos hechos públicos, son de contenido

sexual o erótico, aunque hayan sido obtenidos con el consentimiento, será sancionada con pena de reclusión por un término fijo de cinco (5) años.

Artículo 359.- Hostigamiento, Intimidación o "Cyber-Bullying".

Toda persona que, mediante el uso de cualquier comunicación electrónica oral, escrita, visual o textual, realizada con el propósito de acosar, molestar, intimidar, y afligir a otra persona o a un grupo de personas, ocasione danos a la integridad física, mental o emocional o a la propiedad de la víctima, será sancionada con pena de reclusión por un término fijo de tres (3) años.

Artículo 360.- Intimidación o Amenazas.

Toda persona que, mediante expresiones verbales, escritos, mensajes electrónicos o cualquier otro medio intimide o amenace a una mujer con la que se halle o hubiere estado ligado por relación de consanguinidad, afinidad, sujetos a tutela, cónyuges, excónyuges, convivientes en unión de hecho estable, novios, exnovios, relación de afectividad; con causarle un daño grave y probable de carácter físico, psicológicos, sexual, laboral o patrimonial, será sancionada con pena de reclusión por un término fijo de un (1) año.

Artículo 361.- Calumnia o Injuria.

Toda persona que, impute falsamente a otro la comisión o participación en un delito concreto será sancionada con pena de reclusión por un término fijo de dos (2) años. Si la calumnia se propagara con publicidad, será sancionada con pena de reclusión por un término fijo de tres (3) años.

Artículo 362.- Difamación.

Toda persona que, difame a través de medios electrónicos, informáticos, telemáticos, de telecomunicaciones o audiovisuales, será sancionada con pena de reclusión por un término fijo de cinco (5) años.

Artículo 363.- Extorsión Informática "Ransomware".

Toda persona 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, será sancionada con pena de reclusión por un término fijo de cinco (5) años.

La pena de reclusión será por un término fijo de ocho (8) años, cuando la conducta se realice valiéndose de cualquier manipulación informática, telemática, electrónica o tecnológica.

SECCIÓN QUINTA – DELITOS ECONÓMICOS Y COLECTIVOS

Artículo 364.- Clonación o Uso Fraudulento de Tarjetas de Crédito o Débito.

Las siguientes conductas constituyen delito de uso fraudulento de tarjeta de crédito o débito:

(a) falsificar tarjetas de crédito o débito;

(b) usar, vender, exportar, importar o distribuir tarjetas de crédito o débito falsificadas o sustraídas;

(c) negociar, en cualquier forma, con tarjetas de crédito o débito falsificadas o sustraídas;

(d) usar, vender, exportar, importar o distribuir los datos o el número de una tarjeta de crédito o débito, haciendo posible que terceros realicen

operaciones de compra o de acceso al crédito o al débito que corresponden exclusivamente al titular;

(e) negociar, en cualquier forma, con los datos o el número de la tarjeta de crédito o débito, para las operaciones señaladas en la letra anterior; o

(f) usar maliciosamente una tarjeta bloqueada, en cualquiera de las formas señaladas en las letras precedentes.

La pena de reclusión será por un término fijo de ocho (8) años.

Artículo 365.- Estafa Informática.

Toda persona que, en perjuicio de una persona natural 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, será sancionada con pena de reclusión por un término fijo de tres (3) años.

La pena será de cinco (5) años de reclusión, 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.

La persona que, para obtener un beneficio patrimonial para sí misma o para una tercera persona, mediante la simulación de hechos falsos o la deformación u ocultamiento de hechos verdaderos, induzca a error a otra, con el fin de que realice un acto que perjudique su patrimonio o el de una tercera, será sancionada con pena de reclusión por un término fijo de siete (7) años.

Además, toda persona que, defraude mediante el uso de dispositivos electrónicos que alteren, modifiquen, clonen o dupliquen los dispositivos originales de un cajero automático para capturar, almacenar, copias o reproducir información de tarjetas de crédito, débito, pago o similares, será sancionada con pena de reclusión por un término fijo de diez (10) años.

Artículo 366.- Transferencia Electrónica de Activo Patrimonial.

Toda 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 de reclusión por un término fijo de cinco (5) 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 367.- Apropiación Fraudulenta por Medios Electrónicos.

Toda persona que, utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno, o que

procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena de reclusión por un término fijo de tres (3) años.

Además, será sancionada con pena de reclusión por un término fijo de cinco (5) años, cuando el delito se cometiere con inutilización de sistemas de alarma o guarda, descubrimiento o descifrado de claves secretas o encriptadas, utilización de tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura a distancia, o violación de seguridades electrónicas, informáticas u otras semejantes.

Artículo 368.- Difusión de Información Falsa.

Toda persona que, 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, será sancionada con pena de reclusión por un término fijo de seis (6) años.

Artículo 369.- Pánico Económico o Financiero.

Toda persona que publique, difunda o divulgue noticias falsas que causen daño a la economía nacional para alterar los precios de bienes o servicios con el fin de beneficiar a un sector, mercado o producto específico, será sancionada con pena de reclusión por un término fijo de siete (7) años.

La persona que divulgue noticias falsas que causen alarma en la población y provoquen el retiro masivo de los depósitos de cualquier institución del sistema financiero

y las de la economía popular y solidaria que realicen intermediación financiera, que pongan en peligro la estabilidad o provoquen el cierre definitivo de la institución, será sancionada con pena de reclusión por un término fijo de diez (10) años.

Artículo 370.- Registros Prohibidos.

Toda persona que, sin autorización promueva, facilite, autorice, financie, cree o comercialice un banco de datos o un registro informático con datos que puedan afectar a las personas naturales o jurídicas, será sancionada con pena de reclusión por un término fijo de tres (3) años.

Artículo 371.- Divulgación de Información Financiera Reservada.

Toda persona que, en beneficio propio o de terceros, divulgue información financiera declarada como reservada por el ente rector de finanzas públicas, que genere condiciones económicas desfavorables para el Estado, será sancionada con pena de reclusión por un término fijo de cinco (5) años.

Artículo 372.- Transferencia de Activos.

Toda persona 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, será sancionada con pena de reclusión por un término fijo de cinco (5) años.

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 párrafo anterior, o de una estafa.

Artículo 373.- Sabotaje al Sistema Financiero.

Toda persona que, sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, será sancionada con pena de reclusión por un término fijo de tres (3) años.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, será sancionada con pena de reclusión por un término fijo de cinco (5) años.

Artículo 374.- Delitos Contra la Autoridad.

Toda persona natural o en su caso al representante de la persona jurídica que sea requerida por el Ministerio Público o por la autoridad competente para colaborar o aportar información para la localización geográfica, en tiempo real de los dispositivos de comunicación conforme a las leyes federales o estatales aplicables, que estén relacionados con investigaciones en materia de delincuencia organizada, delitos contra la salud, secuestro, extorsión, amenazas o cualesquiera aplicables y que se rehusare hacerlo de forma dolosa, será sancionada con pena de reclusión por un término fijo de ocho (8) años.

Las mismas penas se aplicarán a la persona natural, o en su caso al representante de la persona jurídica que de forma dolosa obstaculice, retrase sin justa causa o se rehusé a colaborar en la intervención de comunicaciones privadas, o a proporcionar información a la que estén obligados, en los términos de la legislación aplicable.

SECCIÓN SEXTA – DELITOS CONTRA LA PRUEBA DOCUMENTAL

Artículo 375.- Destrucción o Daño a Documentos o Señales.

Toda persona que, con la intención de perjudicar a otro:

(a) destruyera, dañara, ocultara o de otra forma suprimiera un documento o una traficación técnica, en contra del derecho de otro a usarlo como prueba;

(b) borrara, suprimiera, inutilizara o alterara, en contra del derecho de disposición de otro, con relevancia para la prueba; o

(c) destruyera o de otra forma suprimiera señales destinadas a indicar un límite o la altura de las aguas.

Sera sancionada con pena de reclusión por un término fijo de cinco (5) años.

Artículo 376.- Falsificación de Medios Electrónicos de Pago.

Toda persona que, con la intención de inducir en las relaciones jurídicas al error o de facilitar la inducción a tal error:

(a) falsificare o alterare una tarjeta de crédito o débito u otro medio electrónico de pago; o

(b) adquiera para sí o para un tercero, ofreciere, entregare a otro o utilizare tales tarjetas o medios electrónicos.

Será sancionada con pena de reclusión por un término fijo de cinco (5) años.

Cuando el autor actuare comercialmente o como miembro de una organización criminal dedicada a la realización de los hechos punibles señalados, será sancionada con pena de reclusión por un término fijo de siete (7) años."

Sección 2.- Se eliminan los actuales Artículos 301, 302, 303, 304, 305, 306, 307, 308 y 309 de la Ley Núm. 146-2012, según enmendada, conocida como el "Código Penal de Puerto Rico".

Sección 3.- Aplicabilidad.

La conducta realizada con anterioridad a la vigencia de esta Ley en violación a las disposiciones del Código Penal vigente o de cualquier otra ley especial de carácter penal se regirá por las leyes vigentes al momento del hecho.

Si esta Ley suprime algún delito no deberá iniciarse el encausamiento, las acciones en trámite deberán sobreseerse, y las sentencias condenatorias deberán declararse nulas y liberar a la persona. Sólo se entenderá que un delito ha sido suprimido cuando la conducta imputada no constituiría delito alguno bajo esta Ley y el Código Penal vigente. El hecho de que se le cambie el nombre o denominación a un delito, o que se modifique la tipificación del mismo no constituirá la supresión de tal delito.

Sección 4.- Clausula de Separabilidad.

Si cualquier artículo, inciso, parte, párrafo o cláusula de este Código o su aplicación a cualquier persona o circunstancia, es declarada inconstitucional por un tribunal, la sentencia dictada no afectará ni invalidará las demás disposiciones, sino que su efecto quedará limitado y será extensivo al artículo, inciso, parte, párrafo o cláusula, o su aplicación, que haya sido declarada inconstitucional.

Sección 5.- Desacato.

Esta Ley no afecta la facultad conferida por ley a cualquier tribunal, agencia, administración o funcionario público para castigar por desacato.

Sección 6.- Delitos no Incorporados.

La inclusión de esta Ley al Código Penal, respecto a algunos delitos o disposiciones previstas en leyes especiales, no implica la derogación de dichas leyes ni de aquellos delitos especiales no incorporados a esta Ley, siempre y cuando no resulten incompatibles con la presente medida.

Sección 7.- Vigencia.

Esta Ley comenzará a regir a los ciento ochenta (180) días después de su aprobación.