LEY ESPECIAL DE CIBERDELITOS

LEY Nº. 1042, aprobada el 27 de octubre de 2020

Publicada en La Gaceta, Diario Oficial Nº. 201 del 30 de octubre de 2020

EL PRESIDENTE DE LA REPÚBLICA DE NICARAGUA

A sus habitantes, hace saber:

Que,

LA ASAMBLEA NACIONAL DE LA REPÚBLICA DE NICARAGUA

Ha ordenado lo siguiente:

LA ASAMBLEA NACIONAL DE LA REPÚBLICA DE NICARAGUA

En uso de sus facultades,

HA DICTADO

La siguiente:

LEY Nº. 1042

LEY ESPECIAL DE CIBERDELITOS

Capítulo I
Disposiciones Generales

Artículo 1 Objeto
La presente Ley tiene por objeto la prevención, investigación, persecución y sanción de los delitos cometidos por medio de las Tecnologías de la Información y la Comunicación, en perjuicio de personas naturales o jurídicas, así como la protección integral de los sistemas que utilicen dichas tecnologías, su contenido y cualquiera de sus componentes, en los términos previstos en esta Ley.

Artículo 2 Ámbito de aplicación
La presente Ley es de orden público y se aplicará a quienes cometan los delitos previstos en ésta, dentro o fuera del territorio nacional.

Artículo 3 Definiciones

Fuente: http://www.leybook.com/doc/25069

Para los efectos de la presente Ley se entenderá:

1. Acceso a sistemas de información: Es la entrada a dicho sistemas, incluyendo los accesos remotos.

2. Acceso a la información contenida en un dispositivo que permita el almacenamiento de datos: Es la lectura, copia, extracción, modificación o eliminación de la información contenida en dicho dispositivo.

3. Copia de datos: Es la reproducción total o parcial de la información digital.

4. Ciberdelitos: Acciones u omisiones, típicas, antijurídicas, continuas o aisladas, de carácter penal, cometidas en contra de personas naturales y/o jurídicas, utilizando como método, como medio o como fin, los datos, sistemas informáticos, Tecnologías de la Información y la Comunicación y que tienen por objeto lesionar bienes jurídicos personales, patrimoniales o informáticos de la víctima.

5. Datos informáticos: Es cualquier representación de hechos, información o conceptos en un formato digital o analógico, que puedan ser generados, almacenados, procesados o transmitidos a través de las Tecnologías de la Información y la Comunicación.

6. Datos relativos al tráfico: Todos los datos relativos a una comunicación realizada a través de cualquier medio tecnológico, generados por este último, que indiquen el origen, el destino, la ruta, la hora, la fecha y el tipo de servicio o protocolo utilizado, tamaño y la duración de la comunicación.

7. 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.

8. Datos personales sensibles: Es toda información privada que revele el origen racial, étnico, filiación política, credo religioso, filosófico o moral, sindical, relativo a su salud o vida sexual, antecedentes penales o faltas administrativas, económicos financieros; así como información crediticia y financiera y cualquier otra información que pueda ser motivo de discriminación.

9. 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.

10. Dispositivos de almacenamiento de datos informáticos: Es cualquier medio 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.

Fuente: http://www.leybook.com/doc/25069

11. Entrega de datos y archivos informáticos: Se entiende la transferencia de informaciones, documentos o datos en formato electrónico que obren en poder de particulares, entidades públicas o privadas.

12. Identidad informática: Información, datos o cualquier otra característica que individualice, identifique o distinga una persona de otra o a un usuario de otro usuario, dentro de un sistema informático.

13. Incautación y depósito de sistemas informáticos o dispositivos de almacenamiento de datos: Se entiende su ocupación física y su aseguramiento por las autoridades competentes.

14. Interceptar: Acción de apropiarse o interrumpir datos informáticos contenidos o transmitidos por medio de las Tecnologías de la Información y la Comunicación antes de llegar a su destino.

15. Interferir: Obstaculizar, perturbar u obstruir por medio de las Tecnologías de la Información y la Comunicación los sistemas informáticos, públicos o privados.

16. Intervención de comunicaciones a través de las Tecnologías de la Información y la Comunicación: Se entiende la captación, escucha o grabación en tiempo real del contenido de dichas comunicaciones sin interrupción de las mismas, así como de los datos de tráfico.

17. Pornografía infantil: Comprende cualquier representación de la imagen o voz de un niño, niña o adolescente, realizando actividades sexuales o eróticas, implícitas o explícitas, reales o simuladas, así como la exposición de sus partes genitales, con fines sexuales, por cualquier medio sea directo, mecánico, digital, audio visual, o con soporte informático, electrónico o de otro tipo.

18. Persona con discapacidad necesitada de especial protección: Aquella persona con discapacidad que tenga o no judicialmente modificada su capacidad de obrar, requiera de asistencia o apoyo para el ejercicio de su capacidad jurídica y para la toma de decisiones respecto de su persona, de sus derechos o intereses a causa de sus limitaciones intelectuales o mentales de carácter transitoria o permanente.

19. Proveedor de servicios: Es la persona natural o jurídica, pública o privada, que suministre a los usuarios servicios de comunicación, seguridad informática, procesamiento o almacenamiento de datos, a través de las Tecnologías de la Información y la Comunicación.

20. Programa informático: Es la herramienta o instrumento elaborado en lenguaje informático que ejecuta una secuencia de procesos en un sistema informático.

21. Requerimiento de preservación inmediata de datos que se hallan en poder

de terceros: Se entiende la imposición a Personas Naturales o Jurídicas del deber de conservación íntegra de la información digital que obre en su poder o sobre la que tenga facultades de disposición.

22. Sellado, precinto y prohibición de uso de sistemas informáticos o dispositivos de almacenamiento de datos: Se entiende su bloqueo o la imposibilidad de su utilización conservando la integridad de su contenido.

23. Sistema informático: Todo dispositivo aislado, conectado o relacionado a otros dispositivos mediante enlaces de comunicación o la tecnología que en futuro la reemplace, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa informático.

24. Tarjeta inteligente: Cualquier dispositivo electrónico que permite la ejecución de cierta lógica programada para el almacenamiento de información y/o datos, que se utiliza como instrumento de identificación o de acceso a un sistema, para realizar gestiones electrónicas al titular autorizado.

25. Tecnologías de la Información y la Comunicación: Conjunto de medios de comunicación y las aplicaciones de información que permiten la captura, producción, reproducción, transmisión, almacenamiento, procesamiento, tratamiento, y presentación de información, en forma de imágenes, voz, textos, códigos o datos contenidos en señales de naturaleza acústica, óptica o electromagnética, entre otros, por medio de protocolos de comunicación, transmisión y recepción.

Capítulo II
Delitos Relacionados con la Integridad de los Sistemas Informáticos

Artículo 4 Acceso indebido a sistemas informáticos
El que intencionalmente y sin autorización o excediendo la que se le hubiere concedido, acceda, intercepte o haga uso parcial o totalmente de un sistema informático que utilice las Tecnologías de la Información y la Comunicación, será sancionado con prisión de uno a tres años y doscientos a quinientos días multa.

Artículo 5 Acceso indebido a los programas o datos informáticos
El que a sabiendas y con la intención de usar cualquier dispositivo de la Tecnología de la Información y la Comunicación, accediera directa o indirectamente, 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 y trescientos a quinientos días multa.

Las penas para las conductas descritas en los Artículos 4 y 5, se incrementarán en un tercio en su límite inferior y superior, cuando se cometan con fines comerciales o en contra de:

1. Oficinas públicas o bajo su tutela.

2. Instituciones públicas, privadas o mixtas que prestan un servicio público.

3. Bancos, instituciones de micro finanzas, almacenes generales de depósitos, grupos financieros, compañías de seguros y demás instituciones financieras y bursátiles supervisadas y/o reguladas en Nicaragua.

Artículo 6 Interceptación de comunicaciones y trasmisiones entre sistemas de las Tecnologías de la Información y la Comunicación
La persona que ilegítimamente intercepte cualquier tipo de comunicación escrita que no le esté dirigida, o que utilizando las Tecnologías de la Información y la Comunicación intercepte cualquier transmisión, hacia, desde o dentro de un sistema informático o cualquier medio tecnológico que no esté disponible al público; o las emisiones electromagnéticas que están llevando datos de un sistema informático, será sancionada con prisión de uno a tres años y doscientos a quinientos días multa.

Artículo 7 Captación indebida de comunicaciones ajenas a través de las Tecnologías de la Información y la Comunicación
Quien ilegítimamente, haciendo uso de las Tecnologías de la Información y la Comunicación, o de cualquier otro medio, grabe o capte las palabras o conversaciones ajenas, sean éstas video, imágenes, códigos, audio o texto, no destinadas al público, escuche o intervenga comunicaciones privadas que no le estén dirigidas, será penado con prisión de uno a tres años y cien a trescientos días multa.

Artículo 8 Interferencia del sistema informático o datos
El que intencionalmente y por cualquier medio interfiera o altere el funcionamiento de un sistema informático o los datos contenidos en él, de forma temporal o permanente, será sancionado con prisión de tres a cinco años y doscientos a cuatrocientos días multa.

Si la conducta anterior afectare a los sistemas informáticos del Estado, o aquellos destinados a la prestación de servicios de salud, comunicaciones, financieros, energía, suministro de agua, medios de transporte, puertos y aeropuertos, seguridad ciudadana, sistema de seguridad social, educación en cualquiera de sus subsistemas y defensa nacional u otros de servicio al público, la sanción de prisión será de cuatro a seis años y trescientos a quinientos días multa.

Artículo 9 Alteración, daño a la integridad y disponibilidad de datos
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 cuatro a seis años y trescientos a quinientos días multa.

Fuente: http://www.leybook.com/doc/25069

Artículo 10 Daños a sistemas informáticos
El que destruya, dañe, modifique, ejecute un programa o realice cualquier acto que altere el funcionamiento o inhabilite parcial o totalmente un sistema informático que utilice las Tecnologías de la Información y la Comunicación o cualquiera de los componentes físicos o lógicos que lo integran, será sancionado con prisión de tres a cinco años y trescientos a quinientos días multa.

Si el delito previsto en el párrafo anterior se cometiere por imprudencia será sancionado con doscientos a quinientos días multa.

Si el delito previsto en el presente artículo recayera en contra de cualquiera de los componentes de un sistema informático que utilicen las Tecnologías de la Información y la Comunicación, que estén destinadas a la prestación de servicios públicos o financieros, o que contengan datos personales, datos personales sensibles, información pública reservada, técnica o propia de personas naturales o jurídicas, la sanción de prisión será de cuatro a seis años y trescientos a seiscientos días multa.

Si la acción prevista en el párrafo anterior se cometiere por imprudencia será sancionado con trescientos a seiscientos días multa.

Artículo 11 Posesión de equipos o prestación de servicios para vulnerar la seguridad informática
El que posea, produzca, facilite, adapte, importe, venda equipos, dispositivos, programas informáticos, contraseñas o códigos de acceso con el propósito de vulnerar, eliminar ilegítimamente la seguridad de cualquier sistema informático, ofrezca o preste servicios destinados a cumplir los mismos fines para cometer cualquiera de los delitos establecidos en la presente Ley, será sancionado con prisión de cuatro a seis años y trescientos a seiscientos días multa.

Capítulo III
De los Delitos Informáticos

Artículo 12 Fraude informático
El que por medio del uso indebido de las Tecnologías de la Información y la Comunicación, valiéndose de cualquier manipulación de los sistemas informáticos o cualquiera de sus componentes, datos informáticos o información en ellos contenida, consiga insertar instrucciones falsas o fraudulentas que produzcan un resultado que permita obtener un provecho para sí o para un tercero en perjuicio ajeno, será sancionado con prisión de tres a seis años y trescientos a seiscientos días multa.

Artículo 13 Espionaje informático
Quien indebidamente obtenga datos personales sensibles o información pública reservada contenida 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 y trescientos a seiscientos días multa.

Fuente: http://www.leybook.com/doc/25069

Si alguna de las conductas descritas anteriormente se cometieren con el fin de obtener beneficio para sí o para otro, se pusiere en peligro la seguridad soberana 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 la información pública clasificada como reservada de conformidad a la ley de la materia, la sanción será de seis a diez años de prisión y trescientos a seiscientos días multa.

Artículo 14 Violación de la seguridad del sistema informático
La persona que sin poseer la autorización correspondiente transgreda la seguridad de un sistema informático restringido o protegido, será sancionada con prisión de dos a cinco años y trescientos a seiscientos días multa.

Igual sanción se impondrá a quien induzca a un tercero para que de forma involuntaria realice la conducta descrita en el párrafo anterior.

Artículo 15 Hurto por medios informáticos
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 patrimonial, sustrayéndolos a su propietario, tenedor o poseedor, con el fin de obtener un provecho económico para sí o para otro, siempre que el valor de lo hurtado sea mayor a la suma resultante de dos salarios mínimos mensuales del sector industrial será sancionado con prisión de dos a cinco años y trescientos a seiscientos días multa.

Capítulo IV
Delitos Informáticos Relacionados con el Contenido de los Datos

Artículo 16 Manipulación de registros
Quien abusando de sus funciones de administración de plataformas tecnológicas, públicas o privadas, deshabilite, altere, oculte, destruya, o inutilice en todo o en parte cualquier información, dato contenido en un registro de acceso o uso de los componentes de éstos, se le impondrá pena de cinco a ocho años de prisión y trescientos a seiscientos días multa.

Si las conductas descritas anteriormente favorecieren la comisión de otro delito por un tercero, la pena se agravará hasta en un tercio en su límite inferior y superior.

Artículo 17 Manipulación fraudulenta de tarjetas inteligentes o instrumentos similares
El que intencionalmente y sin la debida autorización por cualquier medio crea, 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, se le impondrá pena de cinco a ocho años de prisión y trescientos a seiscientos días multa.

Fuente: http://www.leybook.com/doc/25069

Artículo 18 Obtención indebida de bienes o servicios por medio de tarjetas inteligentes o medios similares
El que sin autorización, haciendo uso de las Tecnologías de la Información y la Comunicación, utilice una tarjeta inteligente ajena o instrumento destinado a los mismos fines, para la obtención de cualquier bien o servicio o para proveer su pago sin erogar o asumir el compromiso de pago de la contraprestación debida obtenida, se le impondrá pena de cinco a ocho años de prisión y trescientos a seiscientos días multa.

Artículo 19 Provisión indebida de bienes o servicios
Quien a sabiendas que una tarjeta inteligente o instrumento destinado a los mismos fines, se encuentra vencido, revocado, se haya indebidamente obtenido, retenido, falsificado o alterado; provea a quien los presente de dinero, efectos, bienes o servicios, o cualquier otra cosa de valor económico se le impondrá pena de cinco a ocho años de prisión y trescientos a seiscientos días multa.

Artículo 20 Violación de la custodia judicial de datos
Quien a sabiendas que un sistema informático o cualquiera de sus componentes se encuentra bajo custodia judicial y haga uso de éstos, manipule sus registros o contenidos, violente los precintos o sellados, se le impondrá una pena de uno a cuatro años de prisión.

Si la acción descrita en el párrafo anterior fuere realizada, facilitada o permitida por el encargado de la custodia judicial se le impondrá una pena de dos a cinco años de prisión.

Artículo 21 Falta a la confidencialidad
Quien faltare a la confidencialidad sobre la información que conoció en ocasión de su participación en el proceso de investigación, recolección, interceptación o intervención de datos de un sistema informático o de sus componentes, se le impondrá pena de cien a trescientos días multa.

Artículo 22 Suplantación y apropiación de identidad informática
El que suplantare o se apoderare de la identidad informática de una persona natural o jurídica por medio de las Tecnologías de la Información y la Comunicación, se le impondrá pena de tres a cinco años de prisión y doscientos a quinientos días multa.

Si con las conductas descritas en el párrafo anterior se daña, extorsiona, defrauda, injuria o amenaza a otra persona para ocasionar perjuicio u obtener beneficios para sí mismo o para terceros, se le impondrá pena de cinco a ocho años de prisión y trescientos a seiscientos días multa.

Artículo 23 Divulgación no autorizada
El que sin autorización da a conocer un código, contraseña o cualquier otro medio de acceso a un programa, información o datos almacenados en un equipo o dispositivo

tecnológico, con el fin de lucrarse a sí mismo, a un tercero o para cometer un delito, se le impondrá pena de cinco a ocho años de prisión y doscientos a quinientos días multa.

Artículo 24 Utilización de datos personales
El que sin autorización utilice datos personales 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, se le impondrá pena de cuatro a seis años de prisión y doscientos a quinientos días multa.

La sanción aumentará hasta en una tercera parte del límite superior de la pena prevista en el párrafo anterior a quien proporcione o revele a otro, información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar.

Artículo 25 Transferencia de información pública reservada
El que sin autorización o excediendo la que se le hubiere concedido, transfiera información Pública clasificada como reservada, de conformidad con la ley de la materia y que mediante el uso de esa información vulnere un sistema o datos informáticos o se pusiere en peligro la seguridad soberana del Estado, apoyándose en cualquier clase de las Tecnologías de la Información y la Comunicación, se le impondrá pena de cinco a ocho años de prisión y doscientos a quinientos días multa.

Artículo 26 Revelación indebida de datos o información de carácter personal
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, sean éstos en imágenes, vídeo, texto, audio u otros, obtenidos por medio de las Tecnologías de la Información y la Comunicación, se le impondrá pena de tres a seis años de prisión y doscientos a quinientos días multa.

Si alguna de las conductas descritas en el párrafo anterior, se hubiese realizado con ánimo de lucro, facilitare la comisión de otro delito o se difunda material sexual explícito en perjuicio de un tercero, se le impondrá pena de cuatro a ocho años de prisión y doscientos a quinientos días multa.

Se impondrá el límite máximo de la pena del párrafo anterior, aumentado hasta en una tercera parte, si alguna de las conductas descritas en el presente artículo, recae sobre datos personales sensibles.

Artículo 27 Suplantación informática en actos de comercialización
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, se le impondrá pena de tres a cinco años de prisión y doscientos a quinientos días multa.

La conducta descrita en el párrafo 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.

Artículo 28 De las amenazas a través de las Tecnologías de la Información y la Comunicación
Quien amenace a otro a través del uso de las Tecnologías de la Información y la Comunicación con:

1. Causar a él, a su familia o a otras personas con las que esté relacionado, un mal que constituya delito y que por su naturaleza parezca verosímil, se le impondrá pena de uno a tres años de prisión.

2. Hacer imputaciones contra el honor, o el prestigio, violar o divulgar secretos, con perjuicio para él, su familia, otras personas con la que esté relacionado, o entidad que representa o en que tenga interés, se le impondrá pena de dos a cuatro años de prisión.

Si la amenaza se hiciera en nombre de entidades o grupos reales o supuestos, se impondrá pena de tres a cinco años de prisión.

Si la amenaza de un mal que constituya delito fuese dirigida a atemorizar a los habitantes de una población, grupo étnico, cultural o religioso, colectivo social o a cualquier otro grupo de personas y tuvieran la capacidad necesaria para conseguirlo, se impondrá pena de cuatro a seis años de prisión.

Artículo 29 Provocación, apología e inducción a la comisión de delitos a través de las Tecnologías de la Información y la Comunicación
Quien, haciendo uso de las Tecnologías de la Información y la Comunicación, incite, instigue, provoque o promueva la comisión de delitos, ensalce el crimen o enaltezca a su autor o partícipes o se lo adjudique, se le impondrá pena de tres a cinco años de prisión y doscientos a quinientos días multa.

Artículo 30 Propagación de noticias falsas a través de las Tecnologías de la Información y la Comunicación
Quien, usando las Tecnologías de la Información y la Comunicación, publique o difunda información falsa y/o tergiversada, que produzca alarma, temor, zozobra en la población, o a un grupo o sector de ella a una persona o a su familia, se impondrá la pena de dos a cuatro años de prisión y trescientos a quinientos días multa.

Si la publicación o difusión de la información falsa y/o tergiversada, perjudica el honor, prestigio o reputación de una persona o a su familia, se le impondrá una pena de uno a tres años de prisión y ciento cincuenta a trecientos cincuenta días multa.

Fuente: http://www.leybook.com/doc/25069

Si la publicación o difusión de la información falsa y/o tergiversada, incita al odio y a la violencia, pone en peligro la estabilidad económica, el orden público, la salud pública o la seguridad soberana, se le impondrá pena de tres a cinco años de prisión y quinientos a ochocientos días multa.

Capítulo V
Delitos Informáticos Relacionados con la Libertad e Integridad Sexual

Artículo 31 Utilización de niñas, niños, adolescentes o personas con discapacidad necesitada de especial protección, en pornografía a través del uso de las Tecnologías de la Información y la Comunicación
Quien, por medio del uso de las Tecnologías de la Información y la Comunicación, induzca, facilite, promueva, utilice, abuse o explote con fines sexuales o eróticos a niñas, niños, adolescentes o personas con discapacidad necesitada de especial protección, haciéndola presenciar o participar en un comportamiento, espectáculo o acto sexual público o privado, se le impondrá pena de cinco a ocho años de prisión y trescientos a seiscientos días multa.

No se reconoce, en ninguno de los supuestos descritos en el párrafo anterior, valor al consentimiento de la víctima.

Artículo 32 Corrupción a personas menores de 16 años o personas con discapacidad necesitada de especial protección a través del uso de las Tecnologías de la Información y la Comunicación
Toda persona mayor de 18 años que haga propuestas implícitas o explícitas a personas menores de 16 años o personas con discapacidad necesitada de especial protección 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 o para terceros, se le impondrá pena de uno a tres años de prisión.

Artículo 33 Acoso a través del uso de las Tecnologías de la Información y la Comunicación
Quien atormente, hostigue, humille, insulte, denigre u otro tipo de conducta que afecte la estabilidad psicológica o emocional, ponga en riesgo la vida o la integridad física, por medio del uso de las Tecnologías de la Información y la Comunicación, se le impondrá pena de dos a cuatro años de prisión.

Cuando la víctima sea niña, niño, adolescente o persona con discapacidad necesitada de especial protección, se impondrá pena de cuatro a seis años de prisión.

Artículo 34 Acoso sexual a través del uso de las Tecnologías de la Información y la Comunicación
Cuando una persona mayor de edad, envíe mensajes, frases, fotografías, vídeos u otra acción inequívoca de naturaleza o contenido sexual a otra persona sin su

consentimiento a través del uso de las Tecnologías de la Información y la Comunicación se le impondrá pena de dos a cuatro años de prisión.

Cuando la víctima sea menor de 16 años, con o sin su consentimiento o persona con discapacidad necesitada de especial protección se le impondrá pena de cuatro a seis años de prisión.

Artículo 35 Condiciones agravantes comunes
Los delitos referidos a los Artículos 31, 32, 33 y 34 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:

1. Ascendientes, descendientes, hermanos, cónyuges, conviviente y familiares hasta el cuarto grado de consanguinidad y segundo de afinidad;

2. Autoridad, funcionarios y empleados públicos;

3. La persona encargada de la tutela, protección o vigilancia de la víctima; y

4. Toda persona que prevaliéndose de la superioridad originada por relaciones de confianza, educativa, de trabajo o cualquier otra relación.

Capítulo VI
Procedimiento, Medidas Cautelares y Procesales

Artículo 36 Investigación, obtención y preservación de datos
En la investigación, obtención y preservación de los datos contenidos en un sistema de información o sus componentes, datos de tráfico, conexión, acceso o cualquier otra información de utilidad, se aplicará lo establecido en la presente Ley.

Artículo 37 Conservación de datos
La Policía Nacional o el Ministerio Público, en el ámbito de su competencia, actuarán con la celeridad requerida para conservar los datos contenidos en un sistema de información o sus componentes, o los datos de tráfico del sistema, principalmente cuando éstos sean vulnerables a su pérdida o modificación.

Artículo 38 Medidas de aseguramiento
Sin perjuicio de cualesquiera otras medidas de aseguramiento que pudieran contribuir a la persecución efectiva de los delitos comprendidos dentro del ámbito de aplicación de esta Ley, se podrán solicitar las siguientes medidas específicas:

1. La incautación y depósito de sistemas informáticos o dispositivos de almacenamiento de datos.

2. El sellado, precinto y prohibición de uso de sistemas informáticos o dispositivos de almacenamiento de datos.

3. El requerimiento de preservación inmediata de datos que se hallen en poder de terceros.

4. La copia de datos.

Artículo 39 Solicitud de autorización judicial
En la etapa de investigación para la obtención y conservación de la información contenida en los sistemas informáticos o cualquiera de sus componentes, se requerirá autorización judicial por cualquier Juez de Distrito de lo Penal, a petición debidamente fundamentada por la Policía Nacional o el Ministerio Público. Una vez iniciado el proceso, cualquiera de las partes podrá solicitar la autorización al Juez de la causa.

Para tal efecto, el Juez podrá:

1. Ordenar a una persona natural o jurídica la entrega inmediata de la información que se encuentre en un sistema de información o en cualquiera de sus componentes;

2. Ordenar a una persona natural o jurídica preservar y mantener la integridad de un sistema de información o de cualquiera de sus componentes, conservar los datos de tráfico, conexión, acceso o cualquier otra información que se encuentre en su poder o bajo su control y que pueda ser de utilidad a la investigación, por un período de hasta noventa (90) días, pudiendo esta orden ser renovada una sola vez por el mismo plazo;

3. Ordenar el acceso a dicho sistema de información o a cualquiera de sus componentes;

4. Ordenar a un proveedor de servicios suministrar información de los datos relativos a un usuario que pueda tener en su posesión o control;

5. Tomar en secuestro o asegurar un sistema de información o cualquiera de sus componentes, en todo o en parte;

6. Realizar y retener copia del contenido del sistema de información o de cualquiera de sus componentes;

7. Ordenar el mantenimiento de la integridad del contenido de un sistema de información o de cualquiera de sus componentes;

8. Hacer inaccesible o remover el contenido de un sistema de información o de cualquiera de sus componentes, que haya sido accedido para la investigación;

9. Ordenar a la persona que tenga conocimiento acerca del funcionamiento de un

sistema de información o de cualquiera de sus componentes o de las medidas de protección de los datos en dicho sistema, a proveer la información necesaria para realizar las investigaciones correspondientes;

10. Ordenar la extracción, recolección o grabación de los datos de un sistema de información o de cualquiera de sus componentes, a través de la aplicación de medidas tecnológicas;

11. Ordenar al proveedor de servicios, recolectar, extraer o grabar los datos relativos a un usuario, así como el tráfico de datos en tiempo real, a través de la aplicación de medidas tecnológicas;

12. Realizar la intervención o interceptación de las telecomunicaciones en tiempo real, según el procedimiento establecido en el artículo 62 de la Ley Nº. 735, Ley de Prevención, Investigación y Persecución del Crimen Organizado y de la Administración de los Bienes Incautados, Decomisados y Abandonados, el cual será aplicable a los delitos contenidos en la presente Ley;

13. Ordenar cualquier otra medida aplicable a un sistema de información o sus componentes para obtener los datos necesarios y asegurar la preservación de los mismos.

Si la autorización es decretada luego de celebrada la Audiencia Preliminar o la Inicial, según se trate, el defensor deberá ser notificado y tendrá derecho a estar presente en la práctica del acto.

En casos de urgencia para realizar el acto de investigación, se procederá de conformidad al Artículo 246 del Código Procesal Penal.

Artículo 40 Competencia Objetiva
En los delitos relacionados en el Capítulo V "Delitos Informáticos relacionados con la Libertad e Integridad Sexual" de la presente Ley, cuando sean cometidas contra mujeres, niñas, niños o adolescentes o personas con discapacidad necesitadas de especial protección, serán competentes para conocer y resolver en primera instancia los Juzgados de Distritos especializados en violencia.

Artículo 41 Responsabilidad del custodio judicial de sistemas informáticos
A quien se le haya confiado la preservación del sistema informático o de cualquiera de sus componentes, así como de su contenido, conservará la confidencialidad e integridad de los mismos, impidiendo que terceros, fuera de las autoridades competentes, tengan acceso y conocimiento de ellos.

Asimismo, la persona encargada de la custodia no podrá hacer uso del sistema de información o de cualquiera de sus componentes en custodia para fines distintos a los concernientes al proceso investigativo.

Fuente: http://www.leybook.com/doc/25069

Artículo 42 Confidencialidad del proceso investigativo
Los que participen en el proceso de investigación, recolección, interceptación, intervención de datos de un sistema de información o de sus componentes, mantendrán en confidencialidad toda la información que conociere sobre la ejecución de los actos realizados por parte de la autoridad competente.

Capítulo VII
Cooperación Internacional

Artículo 43 La extradición
Para efectos de extradición relacionada a la comisión de los delitos tipificados en la presente Ley, a falta de Tratados o Convenios Internacionales de los cuales la República de Nicaragua sea Estado parte, las condiciones, el procedimiento y los efectos de la extradición estarán determinados por lo dispuesto en la Ley Nº. 406, Código Procesal Penal, lo cual se aplicará también a los aspectos que no hayan sido previstos por el Tratado o Convenio respectivo.

Artículo 44 De la asistencia legal mutua
Las autoridades competentes de la República de Nicaragua podrán prestar o solicitar cooperación internacional o asistencia legal mutua, en las investigaciones y procesos relacionados con la aplicación de la presente Ley, de conformidad con los Convenios o Tratados Internacionales en que Nicaragua sea Estado parte.

A falta de Convenio o Tratado Internacional, podrá prestarse o solicitarse asistencia legal mutua con base en el principio de reciprocidad establecido en el Derecho Internacional.

Capítulo VIII
Disposiciones Finales

Artículo 45 Supletoriedad
Lo no previsto en esta Ley, se regulará por las disposiciones de la Ley Nº. 641, Código Penal, Ley Nº. 406, Código Procesal Penal de la República de Nicaragua, Ley Nº. 735, Ley de Prevención, Investigación y Persecución del Crimen Organizado y de la Administración de los Bienes Incautados, Decomisados y Abandonados; Decreto Nº. 70-2010, Reglamento de la Ley Nº. 735, Ley de Prevención, Investigación y Persecución del Crimen Organizado y de la Administración de los Bienes Incautados, Decomisados y Abandonados; Ley Nº. 779, Ley Integral contra la Violencia hacia las Mujeres y de reforma a la Ley Nº. 641 Código Penal; y Ley Nº. 787, Ley de Protección de Datos Personales, en todo aquello que sea aplicable para garantizar el cumplimiento efectivo de esta Ley.

Artículo 46 Emisión de normativa para la preservación de datos informáticos
El Instituto Nicaragüense de Telecomunicaciones y Correos (TELCOR), emitirá una

normativa para la preservación de datos e informaciones por parte de los proveedores de servicios, en un plazo de 3 meses a partir de la publicación de la presente Ley, en La Gaceta, Diario Oficial.

Artículo 47 Derogaciones
Se derogan los Artículos 192, 193, 194, 198, 245, 246 de la Ley Nº. 641, Código Penal, publicada en La Gaceta, Diario Oficial Nº. 83, 84, 85, 86 y 87 del 5, 6, 7, 8 y 9 de mayo de 2008.

Artículo 48 Publicación y vigencia
La presente Ley, entrará en vigencia 60 días después de su publicación en La Gaceta, Diario Oficial.

Dado en la ciudad de Managua, en el salón de Sesiones de la Asamblea Nacional a los veintisiete días del mes de octubre del año dos mil veinte. **MSP. Loria Raquel Dixon Brautigam,** Primera Secretaria de la Asamblea Nacional.

Por tanto. Téngase como Ley de la República. Publíquese y Ejecútese. Managua, el día veintiocho de octubre del año dos mil veinte. **Daniel Ortega Saavedra,** Presidente de la República de Nicaragua.

Fuente: http://www.leybook.com/doc/25069