UNIVERSIDAD NACIONAL DE INGENIERÍA
Dirección de Área de Conocimiento de
Tecnología de la Información y Comunicación

Trabajo Monográfico para optar al título de Ingeniero en Computación

Tema:

Comparación de la ley especial de ciberdelitos Ley N° 1042 con el derecho informático de otros países en América Latina.

Autores:

Br. Jacqueline Grisella Castillo Hernández

Br. Roberto Carlos González Castro

Tutor:

MSc. Roberto Carlos Alfaro Arriola

Enero del 2024

Managua, Nicaragua

DEDICATORIAS

A Dios, por permitirme llegar a este momento tan especial en mi vida. Por los triunfos y los momentos difíciles que me han enseñado a valorarlo cada día más, A mi madre Silvia Cristina Hernández Calero por ser la persona que me ha acompañado durante todo mi trayecto estudiantil y de vida. – Jacqueline

A mis padres y abuelos, quienes fueron los cuatro pilares fundamentales que hoy me permiten alcanzar este hito en mi carrera profesional, les expreso mi amor y agradecimiento profundos. - Roberto

AGRADECIMIENTOS

Agradezco a Dios por protegerme durante todo mi camino y darme fuerzas para superar obstáculos y dificultades a lo largo de toda mi vida. – Jaqueline

A mi madre, que con su demostración de una madre ejemplar me ha enseñado a no desfallecer ni rendirme ante nada y siempre perseverar a través de sus sabios consejos. – Jacqueline

Al MSc. Adilson Gonzalez por ser mi motivo de inspiracion para alcanzar mis metas academicas. - Roberto

ÍNDICE DE CONTENIDOS

CAPÍTULO I: INTRODUCCIÓN 1

I. INTRODUCCIÓN 1

II. ANTECEDENTES 3

III. JUSTIFICACIÓN 5

IV. OBJETIVOS 6

4.1 Objetivo general 6

4.2 Objetivos específicos 6

CAPÍTULO II: BASE TEÓRICA Y METODOLÓGICA 7

V. MARCO TEÓRICO 7

5.1 Antecedentes de los ciberdelitos 7

5.2 Aspectos generales de los ciberdelitos 12

5.3 Definiciones 13

5.4 Convenio Internacional de Telecomunicaciones en Ginebra 15

5.5 Convenio de Budapest sobre Delitos Cibernéticos 15

5.6 Estrategia de Seguridad de Centroamérica (ESCA) 17

5.7 Estrategia Regional Digital para el Desarrollo de la Sociedad de la Información y el Conocimiento SICA 18

5.8 Evolución de la Ciberdelincuencia en Argentina 18

5.9 Evolución de la Ciberdelincuencia en Chile 20

5.10 Evolución de la Ciberdelincuencia en Costa Rica 21

5.11 Evolución de la Ciberdelincuencia en Nicaragua 22

VI. DISEÑO METODOLÓGICO 24

6.1 Enfoque de la investigación 24

6.2 Corte de la investigación 24

6.3 Métodos de la investigación 24

6.4 Universo 25

6.5 Instrumentos 25

6.6 Plan de análisis 25

CAPITULO III: ANÁLISIS DOCUMENTAL Y RESULTADOS 26

VII. ANÁLISIS DOCUMENTAL 26

7.1 Las leyes contra ciberdelitos en Latinoamérica 26

7.2 Principales aspectos de las leyes sobre ciberdelitos en Nicaragua en comparación con las leyes de Costa Rica, Chile y Argentina 29

7.2.1 Nicaragua 29

7.2.2 Costa rica 30

7.2.3 Chile 31

7.2.4 Argentina 32

7.2.5 Comparación y diferencias de las diversas legislaciones de delitos informáticos entre los países estudiados. 34

VIII. CONCLUSIONES 39

IX. RECOMENDACIONES 41

X. BIBLIOGRAFÍA 42

XI. ANEXOS 45

11.1 Anexo 1. Legislación sobre delitos informativos en Nicaragua. 45

11.2 Anexo 2. Legislación sobre delitos informativos en Costa Rica 58

11.3 Anexo 3. Legislación sobre delitos informativos en Chile. 66

11.4 Anexo 4. Legislación sobre delitos informativos en Argentina. 74

11.5 Anexo 5. Casos en donde se aplico la Ley de Ciberdelito en Nicaragua 77

11.5.1 Insólito: condenaron por “ciberdelitos” a 11 años de cárcel a un campesino de Nicaragua que apenas lee y nunca usó PC ni smartphone 77

11.5.2 Exnovio de tiktoker Salma Flores condenado a 5 años de cárcel y a pagar 21 mil córdobas. 80

CAPÍTULO I: INTRODUCCIÓN

I. INTRODUCCIÓN

Las nuevas tecnologías están cambiando el comportamiento social a un ritmo sin precedentes en la historia humana. En esta nueva era, los individuos desarrollan nuevos hábitos y disfunciones y adquieren nuevas identidades sociales como usuarios que pueden acceder, crear, compartir y modificar información y conocimiento.

Hoy en día, Internet se ha convertido en una herramienta de comunicación, acceso a recursos e intercambio electrónico, lo que tiene importantes consecuencias en diversos campos como la sociedad, la economía, el derecho y la cultura.

Debido al abuso de las tecnologías de la información y la comunicación a través de Internet, han surgido delitos de un nuevo orden, delitos no convencionales, estos son los delitos cibernéticos, en la forma de su ejecución, los cuales son principalmente ataques a programas informáticos, redes, equipos de acceso ilegal para sistemas informáticos, interceptación ilegal de datos informáticos, interferencia funcionamiento de los sistemas informáticos, lo cual comprende un comportamiento criminal.

Sin embargo, también existen otros ciberdelitos que afectan más personalmente a la sociedad los cuales son el fraude electrónico, el fraude, los agravios, los insultos, la difamación, la pornografía infantil, el acoso sexual, el terrorismo, el lavado de dinero, el robo, las mentiras ideológicas, los delitos contra los demás.

Otros delitos como la piratería, uso sin permisos de la propiedad intelectual y todos los delitos que puedan cometerse utilizando las tecnologías informáticas.

Esta investigación representa el interés de conocer a mayor profundidad el fenómeno social y jurídico que envuelve a la Ciberdelincuencia ya que en la actualidad, hoy se pueden encontrar vacíos legales en el ordenamiento jurídico, en cuanto a la disciplina del Derecho Informático, debido a que la informática se mueve

más rápido que la legislación, existen diversas conductas criminales por vías informáticas que escapan de ser consideradas como delito; producto de esta situación los usuarios de internet que son víctimas de ciberataques quedan con cierta incertidumbre a la hora de buscar protección, creándose cierto estado de vulnerabilidad a los usuarios.

Este documento se estructura:

Capítulo I: es la parte introductoria donde se presenta al lector sobre el tema, una breve reseña y el objetivo de la investigación.

Capitulo II: explica las teorías y definiciones de la temática planteada, así como también se concibe el diseño metodológico donde explica la metodología, diseño e instrumentos utilizados para la investigación.

Capitulo III: detalla el análisis de los documentos recopilados para la investigación documental, así mismo las conclusiones y recomendaciones.

II. ANTECEDENTES

Internet es el vehículo perfecto para el anonimato, por lo que las identidades digitales actuales, que son "una colección de características de un usuario o grupo de usuarios en un medio transmitido digitalmente", no son confiables porque pueden robarse fácilmente para robar una identidad existente o crear uno nuevo con información falsa.

Anteriormente, en la primera forma de comunicación, las señales ocultas de una persona que usaba dichos servicios eran lo suficientemente pequeñas como para identificar fácilmente si el remitente era falso, por ejemplo, una carta enviada por correo ordinario cuya fuente enviaba un mensaje o una llamada telefónica, se identifica la identidad de la persona, se escucha la autenticidad de la voz con la que se quiere hablar y se registra en el sistema el número de dispositivo, como un teléfono móvil hoy en día.

Los perpetradores de este tipo de actividades delictivas suelen tener como objetivo acosar, acechar, amenazar o insultar a otros, acceder y descifrar los sistemas cifrados para apoderarse de la cuenta de cualquier usuario. Los que hacen tales cosas se conocen como "hackers", que se definirán más adelante.

Internet y las redes telemáticas han creado un nuevo concepto más allá del delito informático tradicional conocido como ciberdelito, que se introdujo internacionalmente después de la Convención sobre Ciberdelincuencia de 2001. La sociedad de la información tradicional o típica, facilitada por las tecnologías que ofrece, principalmente Internet. (Quevedo, 2017)

Estos ciberdelitos las cuales son actividades ilícitas planificadas y realizadas utilizando las nuevas tecnologías de la sociedad de la información son específicas y difíciles de detectar y/o sancionar, así como identificar a los responsables de estas actividades ilícitas. Sin embargo, el desarrollo de nuevas tecnologías ha dado a las autoridades gubernamentales poderosas herramientas de investigación, además de brindar las posibilidades al alcance de los delincuentes. Por lo tanto, debe establecerse un delicado equilibrio entre la capacidad del Estado para hacer frente

a la fenomenología emergente del delito y el espacio de exclusión que la configuración constitucional garantiza a todo ciudadano tercero.

En definitiva, con el auge de la ciberdelincuencia, la justicia penal se enfrenta a delitos cada vez más lesivos, que a su vez requieren de los medios procesales necesarios para resolverlos, como tal es el caso de la implementación de la Ley de ciberdelitos Ley N° 1042.

El 28 de septiembre del 2020 se presentó ante la Asamblea Nacional la Iniciativa de Ley Especial de Ciberdelitos que tiene como objetivo fundamental la prevención, la 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 a los sistemas que utilicen estas tecnologías dentro de Nicaragua. (El 19 Digital, 2020)

La ley se divide en cuatro capítulos de la ley que establece delitos relacionados con la integridad de los sistemas informáticos. Tiene que ver también con los delitos relacionados con el contenido de los datos. Y abarca la ley los delitos que tienen que ver con la integridad sexual. (El 19 Digital, 2020)

Así mismo, la ley penalizará la interceptación de comunicaciones o transmisiones entre sistemas tecnológicos de comunicación e información, así como la captación indebida de comunicaciones ajenas.

La interferencia a los sistemas informáticos, o intercepción de los datos informáticos será penados de 3 a 5 años de cárcel, no obstante, la pena se puede aumentar de 4 a 6 años si la afectación es a los sistemas del Estado, sobre todo en áreas sensibles. (El 19 Digital, 2020)

De igual forma la ley contempla las difamaciones, amenazas, noticias falsas y publicaciones de carácter sexual, además de delitos que atenten contra la integridad física de la niñez, la mujer y personas con discapacidad son delitos que establece la iniciativa de ley. (El 19 Digital, 2020)

III. JUSTIFICACIÓN

En Nicaragua, la ciberdelincuencia es un tema prácticamente nuevo, debido a que los ataques cibernéticos han resultado en un cierto porcentaje de sistemas informáticos gubernamentales y de empresas privadas en los últimos años, poniendo en riesgo datos estatales importantes. Esto se debe a que muchos organismos están apenas empezando a familiarizarse con los ciberdelitos y lo que ello implica, y es de suma importancia el que puedan contar con sistemas de seguridad para controlar la vulnerabilidad de sus equipos tecnológicos, lo que los hará menos vulnerables a los ataques cibernéticos actuales.

La razón de esta investigación es presentar las similitudes y diferencias entre la ley nacional contra los ciberdelitos con las leyes de los países con más desarrollo en la doctrina del derecho informático, como es el caso de Argentina, Chile y Costa Rica. Esto debido a que la problemática de la ciberdelincuencia es un fenómeno social nuevo en Nicaragua y en constante crecimiento, lo cual es importante conocer que los operadores de nuestro ordenamiento jurídico entiendan que a nivel latinoamericano también existen legislaciones que promueven la ciberseguridad. Se estudiaron las legislaciones de Costa Rica, Chile y Argentina en comparación con la legislación de Nicaragua, debido a que estos han sido países precursores y pioneros en materia de delitos informáticos a nivel latinoamericano.

La investigación documental proporcionará los medios necesarios para brindar una visión general adecuada de los tipos de delitos, que a su vez facilitarán la aplicación, al tiempo que brindará información oportuna y consistente a toda la comunidad jurídica para llevar justicia de manera rápida y efectiva a quienes cometen los ciberdelitos, y que se evite así la impunidad y dar a las víctimas la justicia que se merecen. (CEPAL, 2014)

También beneficiará a los docentes y estudiantes de la carrera de ciencias jurídicas y de ciencias informáticas de las universidades nicaragüenses, porque fortalecerá los medios pedagógicos ya que se contará con un estudio de la estructura del tipo penal de los ciberdelitos, para hacer más fácil su comprensión y la manera de como poder identificar estos tipos de delitos.

IV. OBJETIVOS

4.1 Objetivo general

Comparar la ley especial de ciberdelitos Ley N° 1042 con el derecho informático de otros países en América latina.

4.2 Objetivos específicos

- Evaluar las similitudes y diferencias entre la ley especial de ciberdelitos Ley N° 1042 de Nicaragua con las legislaciones de Costa Rica, Chile y Argentina qué preceptúan los delitos informáticos con el uso de una tabla comparativa.
- Describir los retos que contienen la ley especial de ciberdelitos Ley N° 1042 al entorno de Nicaragua.
- Presentar el estado actual de la ley de ciberdelitos de Nicaragua con el derecho informático.

CAPÍTULO II: BASE TEÓRICA Y METODOLÓGICA

V. MARCO TEÓRICO

5.1 Antecedentes de los ciberdelitos

En Nicaragua es notable el avance y uso de las tecnologías. La República de Nicaragua propone disposiciones de seguridad en su constitución política; sus sistemas electrónicos y de comunicación y señala que por razones de seguridad: a) En ningún caso es permisible el establecimiento de sistemas que alteren o afecten los sistemas de comunicación nacional. b) Los puntos de comunicación para fines de la defensa nacional en el territorio nacional deberán ser propiedad del Estado. c) El espectro radioeléctrico y satelital es propiedad del Estado nicaragüense y debe ser regulado por el ente regulador, la ley regulará la materia. (Desayes, 2022)

A su vez, con el surgimiento de la informática, el desarrollo de las TIC, la humanidad entera observa la creación del mundo virtual, cuyas actividades se realizan en el Ciberespacio, y se materializan estas con el uso de la computadora, teléfonos móviles, tablets, herramientas que han incursionado en todos los aspectos de la vida diaria de los seres sociales, corporaciones, Naciones o Estados, pero el uso indiscriminado, sin control, ha dado paso al surgimiento de conductas en mala parten, conductas nocivas y delictivas tanto en el ataque a los propios medios informáticos, programas, ordenadores, que tiene como fin atacar propiamente todo lo relacionado a los programas informáticos. (Quezada, 2021)

De igual manera, Nicaragua cuenta con una Ley Especial de Ciberdelitos la cual 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”. (Desayes, 2022). Hay otros delitos que usan la informática como medio y estos son los delitos que de alguna

manera ya se encuentran tipificados en nuestro ordenamiento jurídico, pero que parte de su itercriminis se realiza desde el uso de un ordenador, estos delitos han surgido desde la creación de la informática, los cuales se han venido perfeccionando hasta volverse cada vez más complejos en la actualidad. (Quezada, 2021)

Según Sain (2018) estos delitos surgen desde 1970, donde las primeras conductas indebidas o ilícitas relacionadas con computadoras eran de tipo económico, entre los que se destacaban el espionaje informático, la "piratería" de software, el sabotaje a bases de datos digitalizados y la extorsión.

En relación con el espionaje, estos se llevaban a cabo mediante la extracción de discos rígidos de las computadoras, el robo de diskettes o copia directa de la información de los dispositivos, tanto, así como la absorción de emisiones electromagnéticas que irradia toda computadora para la captación de datos. El espionaje era comercial o industrial, como suele denominarse, siendo sus principales objetivos los programas de computación, los datos de investigación en el área de defensa, la información contable de las empresas y la cartera de direcciones de clientes corporativas. (Quezada, 2021)

Así mismo, la Republica de Nicaragua, posee una Estrategia Nacional de Ciberseguridad, teniendo como objetivos "Garantizar el uso soberano, seguro y confiable del ciberespacio, que permita el aprovechamiento de las TIC como herramienta que contribuya a la paz, la estabilidad, la seguridad y el desarrollo sostenible del país" (Decreto No. 24-2020 Capítulo IV Estrategia Nacional de Ciberseguridad, inciso b, 2020). (Desayes, 2022)

En relación a la piratería de software, la modalidad característica era la copia no autorizada de programas de computadora para su comercialización en el marco del espionaje industrial. Los casos de sabotaje y extorsión informática eran los delitos que más preocupaban organizaciones ante la alta concentración de datos almacenados en formato digital. (Quezada, 2021)

El portal de software de seguridad y antivirus Avast (2020) explica que, en cuanto a los fraudes de tipo financiero, a fines de esa década y principios de los 80, hubo

casos de alteración de archivos de las bases de datos de las empresas y los balances de los bancos para la manipulación de facturas de pagos de salarios.

Casos típicos se realizaban mediante la instalación de dispositivos lectores, en las puertas de entradas de los cajeros automáticos, y teclados falsos, en los mismos, para la copia de los datos de las tarjetas de débito a través de la vulneración de las bandas magnéticas. Esto motivó, por parte de las empresas emisoras, la adopción de chips, en los plásticos, como medida de seguridad (Sieber, 1998).

Sain (2015) afirma lo siguiente:

Fue justamente durante esta época donde comienza la protección normativa de los países europeos a los bienes inmateriales como el dinero electrónico, proceso iniciado por Estados Unidos en 1978. La cobertura legal de las bases de datos de las instituciones bancarias y empresas, resultaba indispensable para la realización de negocios, fundamentalmente contra el robo de información comercial.

Con la apertura global de internet, a mediados de los años noventa, por parte de la administración norteamericana, y el posterior desembarco de empresas y bancos a la red para el desarrollo del comercio electrónico, la industria editorial, discográfica y cinematográfica, comenzó una afrenta contra la multiplicidad de casos de violaciones a los derechos de autor, a partir de la descarga e intercambio en línea de obras digitalizadas, música y películas protegidas bajo leyes de copyright. (Errius, 2018)

Así mismo, bajo la posibilidad de construcción de identidades ficticias que brindan los entornos virtuales en internet, un rebrote de pedofilia inundó la red mediante la distribución de imágenes de pornografía infantil, igualmente el tema de la protección a la intimidad y la privacidad de las personas comenzaron a ser una preocupación a partir del uso de nuevas tecnologías digitales en la red. (Errius, 2018)

En la década de 1980 el advenimiento del correo electrónico trajo consigo las estafas de phishing y el malware transmitido mediante archivos adjuntos. En la década de 1990, los navegadores web se popularizaron en la misma medida que los virus informáticos. La amplia adopción de las redes sociales en la década del

2000 no hizo sino aumentar la ciberdelincuencia, especialmente el robo de datos, dada la naturaleza de estas plataformas. Durante los diez últimos años, las infecciones con malware y el robo de datos han aumentado enormemente, y nada indica que la tendencia vaya a cambiar. (Avast, 2020)

Cabe resaltar que Nicaragua, hasta el momento no cuenta con un órgano especializado en materia de ciberdefensa como tal, sin embargo, posee algunos mecanismos de aspecto jurídico como leyes las cuales son utilizadas como base o iniciativas en materia ciberdefensa, como el caso del Código de Jurisdicción y Previsión social Militar del Ejercito del Nicaragua, el cual expone que el Ejercito puede participar, en coordinación con las instituciones competentes, en la protección a los sistemas de datos, registros informáticos, espectro radioeléctrico y satelital, para evitar alteraciones o afectaciones a los sistemas de comunicación nacional y lo dispuesto para los fines de defensa nacional.

Con la proliferación del concepto de Internet de las cosas, los ciberdelincuentes cuentan con nuevas y creativas formas de atacar. Cada vez se conectan más objetos cotidianos (neveras, lavadoras, aires acondicionados, bombillas, etcétera), lo que crea nuevas vulnerabilidades y oportunidades para los ciberdelincuentes. Los hackers ya han descubierto cómo infiltrarse en un casino a través de una pecera inteligente y cómo implementar ransomware a través de una cafetera. Aún no conocemos qué alcance tendrá el ciberdelito en la era de IoT, pero no cabe duda de que debemos estar muy atentos al surgimiento de nuevas formas de delito Cibernético. (Quezada, 2021)

A nivel nicaragüense, Espinoza (2018) realizo una entrevista al Comisionado Mayor Iván Escobar, Segundo jefe de la Dirección de Investigaciones Económicas (DIE) en el Programa Visión Policial, ha expresado que hablar de los Ciberdelitos es complejo ya que en el mundo actual todo está referido a la tecnología donde están presentes todas las plataformas y servicios por internet.

“La tecnología en esta parte del desarrollo global, Nicaragua no se está quedando atrás en todos los servicios que se han venido estableciendo incluyendo la Policía

y Estado, están de cara a dar y a garantizar un buen servicio a través en línea", especificó el Comisionando Mayor. (Espinoza, 2018)

Igualmente refirió sobre los delincuentes que se dedican a realizar diferentes actos delictivos, quienes también buscan la manera de como estar pendientes de ejecutar sus actividades delictivas.

El jefe Policial explicó que el delincuente comienza a diseñar sus propios mecanismos, con el objetivo de realizar sus actividades delictivas, siendo la plataforma virtual un eje fundamental del desarrollo global, para cada uno de los países, por lo tanto, ellos mismos van a buscar como insertarse en esa plataforma para ejecutar su hecho ilícito. (Espinoza, 2018)

"Vemos el hecho de las estafas, apuestas ilegales, las extorciones, los ciberbulling, los hacking y los bitching, que vienen siendo más que acceder a los ordenadores y la introducción de los correos electrónicos", detalló Escobar. (Espinoza, 2018)

Sin embargo, trasmitió que en Nicaragua se han neutralizado agrupaciones que han querido desarrollarse en este tipo de aspecto "también vemos que esta plataforma virtual ha sido utilizada para la promoción y divulgación de la pornografía infantil como de adulto que es un delito aberrante principalmente y que es el que combatimos a nivel internacional y nacional". (Espinoza, 2018)

A su vez, reiteró que en esta plataforma también se puede encontrar lo relacionado a ventas de diferentes psicotrópicos ya sea droga, cocaína, marihuana, u otro tipo de droga sintética, "estos se hacen a través de pedidos en claves ampliando su campo de acción", amplió. (Espinoza, 2018)

Además, explicó que los Ciberdelitos dependen de tres aspectos fundamentales: primeramente, si la función va con el individuo como tal, si va contra la propiedad o va contra el Gobierno. (Espinoza, 2018)

"En el caso del individuo es ver con relación a sus tarjetas de crédito, a través de compras y cuentas o transferencias bancarias o a través del engaño llamado comúnmente como ingeniería social". (Espinoza, 2018)

Espinoza (2018), también realizo una entrevista al teniente Winston Galeano, Jefe de la Unidad de Ciberdelitos (DIE), el cual aconsejó referente a los comercios o las páginas web, donde se estén visitando, sean estas debidamente establecidas con su respectiva garantía, “ya que por ejemplo al momento de comprar, tienen que haber un reembolso del producto al momento de que no se pueda enviar”, sostuvo.

También refirió que es de mucho interés asegurarnos que las páginas web tienen un certificado en la parte superior, donde escribimos la dirección de la página web “se encuentra un candadito verde, y ahí dice si es seguro o no el sitio, con ellos se confirma si alguna transacción en estos sitios es seguro para dar la numeración de alguna tarjeta”, concluyó. (Espinoza, 2018)

5.2 Aspectos generales de los ciberdelitos

En este subtema se aborda las generalidades del Ciberdelito, se realiza su caracterización, su identificación dentro de las corrientes doctrinarias y teoría del delito del Derecho Penal. Al respecto existen criterios que esta teoría hay que replantearla, revisarla y adaptarla para poder perseguir y combatir desde el sistema de Justicia este delito emergente, ya que el Ciberdelito es una acción muy compleja desde su inicio, por el lugar donde se produce, desde un espacio virtual como es el Ciberespacio que hay que regularlo, la extraterritorialidad, universalidad, competencia u otro temas que habría que redefinir en la teoría de la tipicidad del delito en particular y en la propia teoría del delito en general. (Quezada, 2021)

Cabe señalar que los países del mundo independientemente de los aspectos teóricos que en su momento se ajustaran, se han unido en este combate al Ciberdelito, firmando Convenios y Tratados Internacionales, creando leyes especiales sobre la materia cumpliendo con el principio de legalidad de “Nullum Crimen, Sine Leges” no hay delito sin ley; El Estado de Nicaragua, presidido por el Presidente de la Republica José Daniel Ortega Saavedra ha aprobado el 27 de octubre del 2020, a través de la Asamblea Nacional la Ley 1042. “Ley Especial Sobre Ciberdelitos”. (Quezada, 2021)

Además, bajo está misma lógica, se encuentra la Ley de Seguridad Soberana, la cual establece como uno de sus objetivos, la preservación y protección de la vida de la persona, la familia y la comunidad nicaragüense, los bienes, la democracia directa, participativa y representativa, fundada en el desarrollo económico, político, cultural, social, alimentario, ambiental, tecnológico de la nación nicaragüense, asimismo entre las definiciones o tipos de amenazas se establecen los ataques externos a la seguridad cibernética que alteren o afecten los sistemas de comunicación nacional, añadiendo a su vez el Código Penal de la Republica de Nicaragua el cual en sus Art. 249, 250 y 327 hacen relevancia a medidas que se optan contra aquellos delitos que atenten a la estabilidad de los sistemas informáticos o infraestructuras relacionadas a ello. (Desayes, 2022)

5.3 Definiciones

Con referencia al aspecto general del Ciberdelitos, se abordan la definición o concepto, que como suele suceder los doctrinarios no se ponen de acuerdo, existen conceptos desde las posiciones más conservadoras hasta las más amplias. A continuación, se exponen algunos conceptos:

En ocasión del 10º Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente se elaboraron dos definiciones:

Primero: Ciberdelincuencia en sentido estricto (delito informático). Comprende cualquier comportamiento ilícito realizado mediante operaciones electrónicas que atentan contra la seguridad de sistemas informáticos y de los datos que éstos procesan. (Gercke, 2014)

Segundo: En sentido general, Ciberdelincuencia (delitos relacionados con los computadores) comprende cualquier comportamiento ilícito cometido por medio de un sistema informático o una red de computadores, o relacionado con éstos, incluidos delitos tales como la posesión ilícita y la puesta a disposición o distribución de información mediante sistemas informáticos o redes de computadores. (Gercke, 2014)

Este concepto se considera que esta bastante completo desde la clasificación de los delitos como fin o medio, ya que en su sentido estricto comprende todas aquellas actividades ilícitas dirigidas a atacar a destruir programas, ordenadores, redes, y todos los aspectos relacionados a la informática; en segundo lugar, se refiere a delitos cometidos utilizando los medios informáticos, que pueden ser cualquier delito de los que están tipificados en los Códigos Penales.

Pino (2016) menciona que:

Delincuencia informática es todo acto o conducta ilícita e ilegal que pueda ser considerada como criminal, dirigida a alterar, socavar, destruir, o manipular, cualquier sistema informático o alguna de sus partes componentes, que tenga como finalidad causar una lesión o poner en peligro un bien jurídico cualquiera.

Este concepto, aunque más estricto que el anterior, por su contenido, la comisión de lo delito Cibernéticos se realiza como fin y como medio según el bien jurídico afectado.

La ley 1042, Ley Especial sobre Ciberdelitos, recién aprobada y que forma parte de nuestro ordenamiento Jurídico en su arto. 3 inc. 4. Define el Ciberdelito, de la siguiente manera: 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.” (Quezada, 2021)

La ley 1042, acoge un criterio de realización del ilícito penal tripartito como método, como medio o fin, el nuevo elemento es que incorpora el método que utilizan los sujetos activos para cometer el delito, es decir también persigue las diferentes formas de acceder a la informática a la internet para el robo de datos, para la destrucción de programas como son entre algunos: Malware; ataques basados en el uso de la web; ataques basados en aplicaciones web; denegación de servicio; botnets; phishing; correo basura (spam); ransomware; amenaza interna; daños

físicos, robos o pérdidas; kit de explotación de vulnerabilidades; violación de datos; robo de identidad; fuga de información. (Ganon, 2017)

De acuerdo a lo antes relacionado este elemento es parte de las circunstancias de modo en el tipo penal, es el modus Operamdum utilizado por el sujeto activo de cómo llevar a cabo este tipo de delito.

5.4 Convenio Internacional de Telecomunicaciones en Ginebra

El convenio Internacional de Telecomunicaciones suscripto en Ginebra el 21 de diciembre de 1959, tiene por objetivo “mantener y ampliar la cooperación internacional para el mejoramiento y el empleo racional de toda clase de telecomunicaciones, asimismo favorecer el desarrollo de los medios técnicos y su más eficaz explotación, a fin de aumentar el rendimiento de los servicios de telecomunicación, acrecentar su empleo y generalizar lo más posible su autorización por su público, armonizar los esfuerzos de las naciones para la consecución de estos fines comunes, de igual forma este convenio coordinará los esfuerzos para eliminar toda interferencia perjudicial entre las estaciones de radiocomunicaciones de los diferentes países y mejorar la utilización del espectro de frecuencias radioeléctricas” (Objeto de la Unión, Art.3, Convenio Internacional de Telecomunicaciones 1959). (Toledo y Cruz, 2020).

5.5 Convenio de Budapest sobre Delitos Cibernéticos

La regulación jurídica de la ciberdelincuencia ha atravesado distintas etapas; a partir de los años 80, tanto en Europa como en Estados Unidos surgen las primeras normas jurídicas que regulan y penalizan delitos cometidos mediante el uso de internet; sin embargo el concepto de ciberdelincuencia era muy restringido; así, en el año 1984, en Estados Unidos se dictó la Ley de Fraude y Abuso Informático (CFAA, por sus siglas en inglés) respecto de aquellos casos de fraude, acceso ilegal y vandalismo informático (Toledo y Cruz, 2020).

Esta normativa tipificó siete conductas relativas a acceso ilegal a computadoras; sin embargo, esta norma solo hacía referencia a “ordenadores protegidos”, es decir, aquellos utilizados por instituciones financieras, gobierno federal, o usados en

comercio o comunicaciones con terceros Estados. Ya en los años 90 tanto Europa como América contaban con normativa sobre cibercrímenes cometidos dentro de sus propios países. Esta legislación interna, asumía que las actividades delictivas ocurrirían por completo dentro de las fronteras territoriales de la nación, y que tanto ofensor como víctima, si no eran ciudadanos de la misma nación, estaban a lo menos situados al interior de ella cuando estos ilícitos acaecían (Toledo y Cruz, 2020).

El 23 de noviembre de 2001, en la ciudad de Budapest se suscribe el Convenio de Ciberdelincuencia, quedando abierto para su firma a los Estados miembros del Consejo de Europa, como también para aquellos países que, sin formar parte de este, quisieran adoptar la normativa contenida en él. El Convenio, viene a complementar otros tratados existentes en el Consejo de Europa en materia de cooperación en materia penal, pero manteniendo el foco en dos objetivos principales; en primer lugar, mejorar la eficacia de las investigaciones y procedimientos penales relativos a delitos cometidos a través de la Red, y, por otra parte, permitir la obtención y mantención de la evidencia electrónica obtenida en estas investigaciones, con miras a su inclusión en juicio. (Toledo y Cruz, 2020)

En esencia, el Convenio requiere que los Estados Parte ajusten su normativa interna, de manera que sean conformes con las disposiciones que implementa; de esta forma, requiere, por una parte, incluir los tipos penales enlistados y definidos por el mismo Convenio; y, por otra, dotar a las autoridades que intervienen en la persecución penal, de las facultades y herramientas procedimentales necesarias para investigar la comisión de estos delitos, incluyendo la expansión de capacidades de inteligencia, vigilancia y herramientas; tales como, incautación de bienes, monitoreo de contenido en línea, retención y transferencia de datos e intervención de comunicaciones privadas. (Toledo y Cruz, 2020)

Respecto estas medidas y conforme al ámbito de aplicación establecido por el propio Convenio, dichas instituciones no estarán restringidas a investigaciones por cibercrímenes, sino que serán extensivas a todos aquellos procedimientos en que

existan evidencias contenida en TICs, sin importar la naturaleza del delito mismo. (Toledo y Cruz, 2020)

En cuanto a la inclusión de tipos penales, el Convenio establece 4 categorías:

- Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos,
- Delitos informáticos,
- Delitos relacionados con el contenido, y
- Delitos relacionados con infracciones a la propiedad intelectual y los derechos afines. (Toledo y Cruz, 2020)

El Convenio de Budapest tiene por objetivo “prevenir los actos que pongan en peligro la confidencialidad, la integridad y la disponibilidad de los sistemas, redes y datos, garantizando la tipificación como delito de dichos actos, tal como se definen contra dichos delitos, facilitando su detección, investigación y sanción, tanto al nivel nacional como internacional, y estableciendo disposiciones materiales que permitan una cooperación internacional rápida y fiable”. (Desayes, 2022)

5.6 Estrategia de Seguridad de Centroamérica (ESCA)

La Estrategia de Seguridad de Centroamérica fue creada el 12 de diciembre del 2007 durante la XXXI Reunión Ordinaria de jefes de Estado y de gobierno del SICA, en Guatemala, la cual fue motivada para preservar e impulsar acciones de seguridad regional, el desarrollo sostenible y el fortalecimiento institucional. De igual forma el ESCA tuvo diferentes etapas para fortalecer su contenido, adaptándolas a las nuevas demandas de seguridad en la región, ejemplo de ello fue la Conferencia Internacional de Seguridad de apoyo a la ESCA, ejecutada del 20 al 23 de junio del 2011, con la presencia de más de 50 delegaciones, declarando apoyo absoluto para la búsqueda de mejores soluciones y abordar los problemas de Centroamérica de manera común. (Desayes, 2022)

Los países firmantes de esta estrategia, son Belice, Guatemala, El Salvador, Honduras, Nicaragua, Costa Rica, Panamá y República Dominicana, los cuales, mediante la ESCA, coordinan, fortalecen y gestionan políticas de seguridad que

permitan crear mejores niveles de seguridad en la región, así como mejorar las condiciones internas de cada Estado, para obtener altos índices de estabilidad y orden. (Desayes, 2022)

5.7 Estrategia Regional Digital para el Desarrollo de la Sociedad de la Información y el Conocimiento SICA

La Estrategia Regional Digital del SICA es producto de los compromisos en la Cumbre Mundial de la Sociedad de la Información (CMSI) celebrada en Ginebra en el año 2003, la cual consistió en orientar acciones comunes a construir una sociedad más desarrollada y actualizada en los medios tecnológicos, lo cual aporte a su propio beneficio, contribuyendo a su vez al desarrollo sostenible y los principios de la Carta de las Naciones Unidas. (Desayes, 2022)

Desayes (2022) explica que la presente estrategia tiene por objeto “Proporcionar a los países miembros del SICA un entorno facilitador para que avancen de manera coordinada y armonizada, en la implementación de iniciativas regionales públicas y privadas, donde el diálogo y el intercambio de experiencias promuevan el desarrollo de la sociedad de la información y el conocimiento en la región; contribuyendo al desarrollo económico, político y social en beneficio de la población centroamericana”.

De igual forma se añaden sus prioridades las cuales son establecidas en la Cumbre Extraordinaria de Jefes de Estado y de Gobierno de los países miembros del SICA para el relanzamiento del proceso de la integración centroamericana, celebrada en la ciudad de San Salvador el 20 de julio de 2010, las cuales se agrupan en los cinco grandes pilares cuyos objetivos se describen a continuación: Seguridad Democrática, Cambio Climático y Prensión de Desastres, Integración Social y Lucha contra la pobreza, Integración Económica, y Fortalecimiento Institucional. (Desayes, 2022)

5.8 Evolución de la Ciberdelincuencia en Argentina

Desde hace unos años se viene observando un fuerte aumento en el uso de las tecnologías de la información y comunicación (TIC) en el mundo y, particularmente

en la República Argentina, lo cual tiene como característica principal la afectación en todos los ámbitos de la actuación de los seres humanos y de las infraestructuras críticas (Estado, salud, comunicaciones, transporte, etc.). (Barrios, 2021)

En este crecimiento, se suma la fácil accesibilidad en el alcance de la tecnología, y por consiguiente ante la necesidad de que las personas se comuniquen, aumenta la tendencia al uso de herramientas tecnológicas, como correos electrónicos, redes sociales, etc., lo que a su vez refleja un mayor incremento en el manejo de internet en la vida cotidiana. (Barrios, 2021)

El 4 de junio de 2008 con la sanción de la Ley Nº 26.388 se incorporaron al Código Penal argentino, los llamados delitos informáticos. Asimismo, se reformaron algunos tipos, para agregar nuevas modalidades de comisión mediante los medios electrónicos. (Andrés, 2020)

La ley 26.388 no constituye una ley especial, sino una norma que modifica, sustituye e incorpora figuras típicas a distintos artículos del Código Penal, con el objeto de "regular las conductas que emergen a partir de las nuevas tecnologías, como medios de comisión de delitos previstos en ese Código" (Anzit y colaboradores, 2010). La ley citada tipifica como delitos informáticos: la pornografía infantil por Internet u otros medios electrónicos (art. 128, C. Penal), el acceso no autorizado a un sistema o dato informático de acceso restringido (art. 153, bis, C. Penal), la violación de las comunicaciones electrónicas sin la debida autorización, su revelación indebida o la inserción de datos falsos (arts. 155 y 157 bis, C. Penal), el fraude informático (art. 173, C. Penal), el daño o sabotaje informático (arts. 183 y 184, C. Penal), los delitos contra las comunicaciones (art. 197, C. Penal). (Andrés, 2020)

Esta reforma al Código Penal argentino se basó en las disposiciones del Convenio sobre cibercriminalidad de Budapest del 23/11/2001. Si bien Argentina, no forma parte de la convención, fue invitado a suscribirla. A pesar de que esta ley significó un importante avance en la materia, permitiendo que los operadores judiciales investiguen nuevas conductas disvaliosas que se cometen a través de dispositivos

informáticos existen otras conductas lesivas, como el robo de identidad, que no son tipificadas ni sancionadas por la legislación argentina. (Andrés, 2020)

5.9 Evolución de la Ciberdelincuencia en Chile

Chile es pionero en Latinoamérica en muchos aspectos positivos, pero también es líder en cuanto a la ocurrencia de ataques cibernéticos en toda América Latina, con un 39% de usuarios de internet afectados, seguido por Colombia y Panamá. El estudio hace hincapié en el hecho que los países que lideran este desafortunado ranking se caracterizan por su creciente y estable economía. (Diario Financiero, 2020)

El aumento de la ciberdelincuencia en Chile tiene varias razones, siendo quizás una de las más importantes la ausencia de una legislación actualizada de aborde de buena forma las distintas hipótesis de comisión de este tipo de ilícitos. La ley de delitos informáticos data de 1993, existiendo solamente un complemento en 2005 mediante la publicación de una normativa que sanciona únicamente el uso indebido de tarjetas de crédito o débito, comúnmente conocido como clonación. En este escenario, hay múltiples conductas que hoy no se encuentran recogidas por el legislador, como el mero hacking, el phishing, el pharming, la divulgación de virus y el fraude informático, entre varios. (Diario Financiero, 2020)

Si a la anterior ecuación se le agrega, por un lado, la inexistencia de medidas de seguridad eficientes por parte de las instituciones financieras y operadores en general y, por otro, la estabilidad económica que Chile posee, se transforma en un imán para delincuentes informáticos extranjeros, los cuales están direccionando sus skimmers y teclados hacia Chile, justamente por las razones anteriormente citadas.

Fuera del mejoramiento de las medidas de seguridad, tema en que la SBIF trabaja, urge que Chile ratifique el Convenio sobre la Ciberdelincuencia (Acuerdo de Budapest) del Consejo de Europa, principal instrumento internacional que contiene los estándares mínimos de protección jurídica en materia penal, procesal penal y de cooperación internacional. Desde hace un par de años que la invitación a formar

parte de este tratado está sobre la mesa del Ejecutivo, pero hasta la fecha no hemos sabido de mayores avances. (Diario Financiero, 2020)

5.10 Evolución de la Ciberdelincuencia en Costa Rica

El proceso de interconexión de Costa Rica a las grandes redes de investigación se inició en 1990 con el establecimiento en la Universidad de Costa Rica (en adelante UCR) del primer nodo, de la Red BITNET3 en la región Centroamericana. (Chavarría et al., 2016)

Tres años después, el 26 de enero de 1993, esta conexión costarricense se integró a la Red Internet. Paralelamente, con las conexiones pioneras de la UCR, se estableció la Red Nacional de Investigación de Costa Rica (en adelante CRNET), una red digital que utiliza enlaces de fibra óptica para interconectar las instituciones académicas y de investigación más importantes del país, y proporcionan amplio acceso a la información y recursos computacionales del mundo. (Chavarría et al., 2016)

Estos logros, no solo permiten la conexión instantánea de un gran número de personas con el resto del mundo, sino que introducen en el país por primera vez la tecnología inter redes a gran escala.

En 1994, Radiográfica Costarricense S.A. (RACSA), realizó las inversiones necesarias para responder a las necesidades del mercado en el acceso a este servicio para el sector comercial, que ofrece también servicios a particulares. A principios de julio 1995 entró en operación un dominio de Internet del sector gobierno que interconectó en su primera fase a 12 ministerios. (Chavarría et al., 2016)

En cuanto al número de internautas, se afirma que, en 1999, en Costa Rica la tasa de usuarios en Internet era de 2.7 usuarios por cada cien mil habitantes. En el 2001 esa tasa se duplicó lo que muestra una tendencia importante al aumento de personas conectadas a Internet. Desde su inicio de operación a la fecha, el crecimiento del servicio Internet en Costa Rica ha experimentado un crecimiento constante de más del 10% anual. (Chavarría et al., 2016)

Años posteriores la población empieza a realizar una serie de denuncias referentes a delitos cometidos, valiéndose de tarjetas de crédito y cajeros automáticos, estas fueron interpuestas ante el Ministerio Público, el cual ante la inexistencia de tipos penales específicos intenta de manera poco exitosa, además contraria al principio Nullum crimen, nulla poena sine previa lege (No hay crimen, no hay pena sin previa ley) hacer pasar estos actos como estafas o hurtos. Tales denuncias van en aumento, costando el desembolso de altas sumas de dinero en protección por parte de los ciudadanos, bancos y empresas. (Chavarría et al., 2016)

De lo anterior se puede decir que la utilización de programas anti phising así como de software antivirus es una imperante necesidad, pues el tráfico en la red, ya sea, para fines de entretenimiento, sociales, negocios o académicos, es un riesgo que debe ser contrarrestado.

5.11 Evolución de la Ciberdelincuencia en Nicaragua

El 17 de febrero de 1983 se funda la Universidad Nacional de Ingeniería (en adelante UNI) como un centro de educación superior. Ese mismo año, antes que se declarara el bloqueo económico, Icaza & Asociados, introdujo al país las primeras computadoras Compaq XT, 8086 y 8088, después optó por traer Cannon; mientras que Canadá Business, traía los acer. (Chavarría et al., 2016)

En 1984, luego que se fundara, Compaq lanzó las primeras computadoras 386. Ese mismo año HP5 introduce al mercado mundial las primeras impresoras láser. Entre 1985 y 1986, sistemas de IBM6 son instalados en el Banco Central, Instituto Nicaragüense de Acueducto y Alcantarillado (INAA), Casa Pellas y el Ingenio San Antonio. (Chavarría et al., 2016)

La entrada de esos equipos era muy tímida debido al sistema imperante de la época. Estos equipos instalados en estas empresas e instituciones fueron sustituidos hasta 1992.

Para 1989, ya se tiene conciencia que la Informática es una realidad frente a los nuevos retos que impone el desarrollo y es exigido en la mayoría de las Universidades impartir la clase de Informática, teniendo trasfondo el Lenguaje de

Programación BASIC. Con el cambio de gobierno, hay una transformación curricular en todas las carreras universitarias y se comienza a impartir y tomar en cuenta la computación como herramienta esencial para el desarrollo humano del profesional. (Chavarría et al., 2016)

Se comenzaron a conectar varias universidades al nodo Nicarao y en fin el despegue tecnológico en Nicaragua es irreversible, pero los frutos son vistos hasta cinco años después, cuando egresan los primeros profesionales con nuevos pensum académicos, se fundan empresas que dan el servicio comercial de Internet, nacen empresas desarrolladoras de sistemas y se estrecha la competencia del mercado de computadora.

Desde el 2007 los ataques de hacker en Nicaragua son de miles y contundentes, especialistas informáticos de la UNI, reconocieron que los sistemas informáticos en Nicaragua son vulnerables a cualquier ataque directo que pueden hacer los Hackers. (Chavarría et al., 2016)

En el 2011 se registra el primer ataque de hackers, realizados por quienes se hicieron llamar anonymous, el cual estuvo dirigido meramente hacia 10 Instituciones del gobierno de Nicaragua, entre ellas se encontraban: Ministerio de Hacienda y Crédito Público, Ministerio Defensa, El Instituto de Energía (INE), entre otros. Debido a eso, dichas Instituciones antes mencionadas, quedaron fuera de la red por varias horas. (Chavarría et al., 2016)

Fue a partir de estos ataques que Nicaragua despertó su interés en proteger a sus ciudadanos de estas amenazas informáticas y poner límites a una delincuencia actualmente desbocada en este ámbito.

El Anteproyecto de Ley sobre Delito Informáticos fue creado con el propósito de salvaguardar a los nicaragüenses de ser víctimas de los posibles ataques de los ciberdelincuentes.

VI. DISEÑO METODOLÓGICO

6.1 Enfoque de la investigación

El enfoque de investigación es cualitativo por el carácter reflexivo del análisis documental. En este sentido, los autores Pérez y Blasco señalan que: "la investigación cualitativa estudia la realidad en su contexto natural y cómo sucede, sacando e interpretando fenómenos de acuerdo con las personas implicadas" (2007, p.25). Es así que el énfasis está puesto en la interpretación y comprensión de un fenómeno social y el significado que tiene para los actores, situándolos en un contexto y espacio determinados. Es así que el énfasis está puesto en la interpretación y comprensión de un fenómeno social y el significado que tiene para los actores, situándolos en un contexto y espacio determinados. En la investigación cualitativa, se hace la distinción entre los significados impuestos por el investigador y los generados por los investigados, teniendo especial importancia las percepciones, motivaciones y demás, de los propios sujetos de análisis, que se convierten en las bases de las conclusiones analíticas

6.2 Corte de la investigación

Se clasifica como investigación de corte transversal, porque se tomará la información en un único instante del tiempo.

6.3 Métodos de la investigación

De acuerdo con los objetivos planteados, esta investigación se considera de tipo documental, la cual se define como una serie de métodos y técnicas de búsqueda, procesamiento y almacenamiento de la información contenida en los documentos, en primera instancia, y la presentación sistemática, coherente y suficientemente argumentada de nueva información en un documento científico, en segunda instancia (Tancara, 1993). De este modo, no debe entenderse ni agotarse la investigación documental como la simple búsqueda de documentos relativos a un tema.

6.4 Universo

Derecho informático, área de ciberdelitos y leyes relacionadas directa e indirectamente, en los países de Nicaragua, Argentina, Chile y Costa Rica.

6.5 Instrumentos

Recopilación documental

Como instrumento de recopilación de información se hizo uso de leyes, tesis, informes, así como elaboración de fichas de contenido y bibliográficas.

6.6 Plan de análisis

Con la documentación obtenida, se inició un proceso de selección de acuerdo con las búsquedas impuestas por los tópicos de indagación mediante un análisis de contenido definido como una técnica de investigación que consiste en el estudio de la realidad social del fenómeno estudiado a través del análisis de los documentos explorados.

Posteriormente, se procedió a interpretar los documentos relacionados con los criterios a considerar. Para la interpretación de los artículos, revistas y leyes seleccionados, en primera instancia, se realizó un análisis documental con base a los aspectos de elementos básicos de la información transcrita y examinarlos con el propósito de responder a las distintas cuestiones planteadas en la investigación.

Luego que se recolectará la información, el siguiente paso fue el análisis de los datos recopilados a través de la recopilación documental, esto se realizó con la ayuda del programa de computación Microsoft Office Word 2021, posteriormente se realizó una revisión minuciosa del trabajo y por último se realizaron las conclusiones y recomendaciones.

CAPITULO III: ANÁLISIS DOCUMENTAL Y RESULTADOS

VII. ANÁLISIS DOCUMENTAL

7.1 Las leyes contra ciberdelitos en Latinoamérica

Analizar la incidencia y prevalencia del ciberdelito requiere métodos adicionales y especializados que ofrece la criminología. El análisis de ciberdelincuencia permite recopilar y analizar información sobre características de comportamiento caracterizadas por avances tecnológicos, hiperconectividad, anonimato de programas creados bajo orientación profesional o empírica y/o utilizados para ciberdelincuencia y uso informático de infraestructuras económicas.

En la sociedad, los últimos cambios provocados por las nuevas tecnologías afectan el bienestar económico, social y político. Toda innovación tecnológica conduce a un aumento de las conductas antisociales que la utilizan en beneficio propio y en perjuicio de terceros. El propósito de esta investigación es enfatizar la importancia de las leyes contra ciberdelitos como parte integral de la profesionalización y formación a largo plazo de los operadores de justicia penal con el objetivo de implementar políticas de persecución penal para combatir la rápida propagación de los delitos informáticos. (Barahona, 2021)

A partir de la identificación de los móviles de los delitos informáticos, se pueden realizar interesantes estudios sobre la incidencia de este fenómeno delictivo en nuestra región latinoamericana, tomando como referencia las investigaciones y análisis realizados por expertos europeos y norteamericanos.

Prevenir y ampliar la lucha contra el ciberdelito es una de las prioridades de las distintas autoridades policiales de la región (como la policía de EE.UU. o INTERPOL) de acuerdo con las líneas de actuación establecidas por el Convenio de Budapest y el sistema internacional de coordinación y cooperación en la lucha contra el crimen organizado. (Barahona, 2021)

La ciberdelincuencia es una intimidación sigilosa que crece rápidamente y que puede causar estragos. Esta realidad requiere que los países de la región

latinoamericana armonicen leyes y regulaciones y se actualicen y capaciten constantemente en este tema, incluyendo aspectos importantes relacionados con la detección temprana de redes de ciberdelincuentes organizados o individuos que actúan solos.

Se necesita con urgencia la armonización de las leyes penales sobre delitos cibernéticos en América Central y la coordinación interregional de los organismos encargados de hacer cumplir la ley que permitan compartir bases de datos para enjuiciar, investigar y castigar de manera efectiva los delitos cibernéticos. (Barahona, 2021)

Actualmente, existen algunas iniciativas destacadas en la región centroamericana para monitorear y recopilar datos sobre delitos cibernéticos, como el Observatorio de Delitos Informáticos de Guatemala (OGDI) o Costa Rica, de igual forma, también merece una evocación especial al trabajo que ejecuta el Instituto Panameño de Derecho y Nuevas Tecnologías (IPANDETEC), que también merecen una mención especial y abarcan un tema muy interesante basado en la difusión de conocimientos preventivos en materia de protección de datos. (Barahona, 2021)

Sin embargo, el sistema de justicia penal de nuestra nación necesita experiencia para que sus operadores comprendan los detalles del comportamiento del delito cibernético a fin de continuar implementando un proceso de justicia dinámico que se adapte a la nueva realidad tecnológica en la que vivimos. El delito cibernético requiere no solo especialización en derecho penal, sino también criminología adicional, desde el comportamiento de la víctima y el perpetrador, pasando por la elaboración de perfiles y el análisis geográfico, hasta el desarrollo de políticas de enjuiciamiento del delito cibernético.

La integración interna de las normas específicas de los convenios internacionales y acuerdos de cooperación interregional es sólo un marco conceptual para la armonización del derecho penal para la regulación del delito cibernético en los países de la región centroamericana. Sin embargo, el sistema de justicia penal también necesita coordinar sus actividades desde la base educativa de sus

miembros, y es aquí donde se destaca el aporte de la criminología al conocimiento que brinda como ciencia complementaria al estudio del derecho penal.

La metamorfosis de las condiciones sociales y empresariales a través del uso y abuso de las nuevas tecnologías ha llevado a la expansión de los delitos informáticos, que a su vez se han vuelto más complejos y diversos, requiriendo constantes adecuaciones y modificaciones de las normas penales para sancionar estas actividades. Las nuevas tecnologías acercan a las personas en términos de cooperación y comunicación de datos para prevenir y combatir el crimen organizado transnacional, pero la realidad es que las innovaciones tecnológicas también modifican el comportamiento de las personas, ya sea por la alta competitividad en el mundo laboral o en la sociedad y las relaciones, o porque de la creciente dependencia del entorno tecnológico o por muchas otras razones ajenas y separables de la delincuencia común. De hecho, el comportamiento en el mundo del ciberdelito no se puede estudiar con la misma lente que el crimen convencional, y los modos de participación son mucho más complejos que los modos tradicionales de inducción, complicidad y coordinación tal como los conocemos. (Barahona, 2021)

Estos complejos operativos requieren de un proceso de formación altamente especializado de los operadores de justicia, así como de un proceso de homogeneización del derecho penal para evitar el surgimiento de los llamados “paraisos virtuales de impunidad” para las investigaciones de delitos informáticos en países de la región con poca o ninguna delincuencia. capacidades de prevención y sanción. (Barahona, 2021)

Según las docentes Linde y Aebi (2021) experta en ciberdelincuencia y profesora de criminología en la Universidad Oberta de Catalunya (España), los ciberdelincuentes no siempre pertenecen a un “grupo homogéneo” y su comportamiento puede verse influido por factores muy diferentes y complejos. Al mismo tiempo (autocontrol, estilo de vida, relaciones sociales, situación laboral) también multiplican sus motivaciones (curiosidad, desafío, venganza, lucro, etc.).

7.2 Principales aspectos de las leyes sobre ciberdelitos en Nicaragua en comparación con las leyes de Costa Rica, Chile y Argentina

En cualquier caso, el delito como medio o blanco del ciberdelito requiere una revisión constante de las bases de datos policiales a nivel nacional y regional para analizar estadísticas de incidentes y perfiles de cumplimiento.

7.2.1 Nicaragua

En la situación de Nicaragua, algunas formas de ciberdelincuencia pretenden ser vehículo de actividades delictivas típicas, como la explotación sexual, la pornografía y las relaciones sexuales con jóvenes a cambio de dinero, los delitos de invasión y, en el caso de los delitos contra la libertad comercial, el hurto y delitos de confidencialidad comercial (Ley No. 641 del Código Penal de la República de Nicaragua). Sin embargo, si se toma en cuenta la fecha de entrada en vigencia de la Ley No. 641 de 2009, o Código Penal, la ley penal para delitos cibernéticos fue actualizada tardíamente, a diferencia de otros países centroamericanos que han implementado estrategias para combatir el delito cibernético, incluyendo la inclusión de nuevos tipos penales en la ley penal nacional y la implementación de estrategias de seguridad nacional, por ejemplo, la Ley Especial contra los Delitos Informáticos y Delitos Conexos de El Salvador de 2016 o la Estrategia Cibernética de Seguridad Nacional de Panamá de 2013 de Panamá. (Barahona, 2021)

En la cuestión particular de Nicaragua, la ley específica de ciberdelincuencia (Ley 1042/20) aprobada en octubre de 2020, la cual refleja la falta de análisis de los niveles de ciberdelincuencia a nivel local que se pueden encontrar en los informes estadísticos. Los datos se refieren al año 2009, ya que se carece de información estadística sobre la tasa de criminalidad de cualquier tipo de delito informático, que ya estaba recogido en el Código Penal de 2009. (Barahona, 2021)

El análisis de la información estadística está relacionado con las dos formas de delinquir antes mencionadas, y si los delitos informáticos son el objeto o medio de la comisión de otros delitos, se pueden elaborar definiciones específicas para cada

caso. Además de lo anterior, la investigación criminológica permitirá extraer características relevantes para el perfil de los ciberdelincuentes. Esto requiere una base de datos detallada y actualizada que no deseche la información recopilada por los investigadores y ayude a determinar los motivos de los delincuentes para cometer delitos cibernéticos (Kranenbarg, 2018), ya sea que se utilicen como un medio para cometer otros delitos o son independientes por sí mismos.

7.2.2 Costa rica

Costa Rica ha estado regulando los delitos informáticos desde 2001 mediante la adopción de la Ley no. 8148, por la que se incorporan (artículo 196a), fraude informático (artículo 217a) y alteración de datos y sabotaje informático (229 Bis). (Bonilla, 2019)

En 2012 se promulgó la Ley N° 9048 bajo el título “Reforma del Capítulo VII, Artículo 8 del Código Penal, “Delitos informáticos y delitos conexos”, que revisó los artículos 167, 196, 196 bis, 214, 217 bis y 229. bis, por el que se reforma el artículo 288 del Código Penal. los principales cambios se reflejan en el aumento de las sanciones, incluyendo conductas relacionadas con el uso de redes sociales y medios informáticos. Por su parte, el artículo 229 añadió el párrafo 1. 6) corresponde a “Daño grave” bajo el epígrafe “Delitos contra la propiedad”, que incluía también el artículo 229 ter, que corresponde a “Sabotaje informático”. (Bonilla, 2019)

Finalmente, se añadió el Título VIII al Título VII “Delitos contra la Propiedad” bajo el título “Delitos Informáticos y Materias Conexas”, que regula materias como la usurpación de identidad (230), el espionaje informático (231), la instalación o distribución de programas informáticos maliciosos. (232), falsificación de sitios electrónicos (233), promoción de delitos informáticos (234), narcotráfico y crimen organizado (235) y difusión de información falsa (236). (Bonilla, 2019)

En cuanto a las normas mencionadas en el párrafo anterior, parece ideal crear un nuevo título en el Código Penal, que incluiría “Delitos informáticos y conexos”. Esto se debe a que los bienes jurídicos que protege no son exclusivos de la "infracción patrimonial".

7.2.3 Chile

En Chile, la Ley n. 19.223, que tipifica a las personas involucradas en delitos informáticos, fue publicada en el Diario Oficial el 7 de junio de 1993. Intenta llenar vacíos en la legislación tipificando los delitos informáticos, cubriendo así un fenómeno cada vez más importante: la protección de datos.

No hay una definitiva conceptualización de delito informático en la Ley N° 19.223. No obstante, de su articulado se puede inferir que su finalidad es proteger los datos informáticos y los sistemas que los contienen, y no utilizar los medios tecnológicos como medio para la comisión de delitos comunes (Muñiz, 2001).

Según la historia de la ley (BCN, 1993), en la moción parlamentaria que dio lugar al proyecto de ley, el diputado José Antonio Vieira-Gallo dijo que la legislación debía proteger estos casos accidentales. Usando tecnología informática moderna, hay una clara referencia al almacenamiento de información, pero ninguna referencia a delitos cometidos por medio de computadoras. En el tratamiento, el concepto amplio de delito informático se considera análogo al concepto norteamericano de "ciberdelito" (como un acto típico, ilegal y punible en el que se utiliza o se expone a la influencia una computadora o sus accesorios), que se acerca más al concepto de ciberdelincuencia. Sin embargo, el enfoque inicial tuvo éxito hasta que la ley se publicó en el Diario Oficial.

El primer proyecto de ley de Delitos Cibernéticos inicialmente intentó identificar cuatro argumentos diferentes de delitos cibernéticos, a saber: protección contra el sabotaje informático, protección contra el espionaje informático, protección de datos como un derecho legal y protección contra la divulgación ilegal de datos informáticos, y especulación del Artículo 5. circunstancias agravantes. La comisión responsable de la Cámara de Representantes redactó la versión final de la ley, señalando que los artículos 1 y 3 también se refieren a delitos de sabotaje informático, mientras que los artículos 2 y 4 son números relacionados con el espionaje informático. En cuanto al artículo 5, el entendimiento de la supresión es que el ánimo de lucro está claramente incluido en las disposiciones especiales y este artículo no es necesario (BCN, 1993). Otro artículo, el cuarto, fue sustituido a

pedido de la Asociación Chilena de Empresas de Tecnologías de la Información para cubrir las revelaciones maliciosas, que no fueron consideradas en su momento (Jijena Leiva, 2019).

Siguiendo la distinción anterior, se entiende por daño informático “la destrucción o falla del software, es decir, datos o programas en una computadora, que, según algunos, pueden afectar el soporte físico (hardware) de un sistema informático” (BCN, 1993), contenida en los artículos 1 y 3 de la ley. Por su parte, se entiende por espionaje informático la “adquisición no autorizada de datos almacenados en archivos informáticos, así como la copia ilícita de programas” (BCN, 1993), tal como se define en los artículos 2 y 4 de la ley. Aunque la ley no hace esta distinción ni establece estas definiciones, los tribunales han hecho suya esta distinción.

En la actualidad la Ley n. 19.223 fue derogada y actualmente es utilizada la ley núm. 21.459 que establece normas sobre delitos informáticos, deroga la ley n° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al convenio de Budapest.

7.2.4 Argentina

En Argentina, el organismo de control regulatorio es la Dirección Nacional de Protección de Datos Personales (DNPDP), que depende del presidente del país y actualmente está incluido por decreto en la Agencia de Acceso a la Información pública, que es el organismo que regula la protección de datos personales y el derecho de acceso a la información pública hasta el decreto 1172/03. (Rodríguez, 2021)

La Ley N° 25 326 regula el uso de datos personales en documentos públicos y privados. Dichos datos sólo pueden ser recabados con el consentimiento del titular y debe garantizarse su uso confidencial. Un principio importante en la legislación aplicable es el principio de finalidad, que establece que los datos no deben utilizarse para fines distintos de aquellos para los que fueron recopilados.

A su vez, es necesario recalcar que existen dos lagunas en la legislación nacional vigente en materia de protección de datos personales. Una es que se creó en 2000 y no tiene en cuenta muchas cosas que sucedieron en el desarrollo y la evolución

de Internet, por lo que las reglas deben ampliar esto y definir muchos aspectos de los datos personales en Internet. (Rodríguez, 2021)

Otro punto a mejorar es que privilegia el ámbito judicial frente a la tramitación de denuncias administrativas, lo que puede dar grandes resultados. Al mismo tiempo, el acceso a la justicia tiende a ser limitado para la mayoría de las personas, lo que a menudo implica la contratación de representación o asesoría legal, además, debido a los términos contractuales, de los propietarios de empresas globales de Internet, incluidas Facebook, Instagram y Twitter con base en los EE. UU y designe un tribunal de California como el lugar para resolver posibles demandas o reclamos legales. Esto dificulta que un gran número de extranjeros o grupos de bajos y medianos ingresos ejerzan sus reclamaciones o derechos de defensa. (Rodríguez, 2021)

Por otra parte, los cambios tecnológicos en el almacenamiento de contenido también plantean preocupaciones sobre la protección de datos personales. Una nueva práctica de hospedaje está pasando de dispositivos físicos sin conexión a hospedaje en línea en la "nube". Sin embargo, estos datos están alojados en hardware ubicado principalmente en los Estados Unidos, por lo que cualquier decisión normativa o política sobre esta información estará influenciada por ese país.

Por ejemplo, la UE desalienta el alojamiento de contenido en servidores de EE. UU., argumentando que EE. UU. es un destino inseguro para la información sobre sus ciudadanos. Otra disposición en este sentido es el requisito de que todas las empresas de la UE tengan el papel de un "delegado de protección de datos" en cada empresa. De acuerdo con la legislación de la UE, que está en vigor desde mayo de 2018, esto debe hacerlo un empleado que se registrará y contactará con la autoridad de control de cada país. (Rodríguez, 2021)

Hablando del caso de argentina, las opciones institucionales en este caso tienen temas a considerar, como la Agencia de Acceso Público a la Información (AAIP) apoyándose en el Poder Ejecutivo Estatal (PEN). Por lo tanto, cuando llegue su

turno de reclamar o condenar a PEN, es posible que nunca pueda hacer verdaderamente su parte. (Rodríguez, 2021)

Otro análisis que los expertos consideran destacable es que la ley de acceso a la información pública (que preveía la creación de la AAIP) creó un órgano de control con una estructura similar a la Agencia de Datos Personales, pero que por su nombre y estructura puede ser asume que el acceso a la información pública es menor. La protección de los datos personales o la privacidad es más importante. Para nuestro país, esto puede ser contrario a nuestra tendencia, donde la protección de datos personales es un requisito previo para los otros dos derechos.

Actualmente los delitos informáticos están regidos por la ley Nacional N° 26.388 de Delitos Informático, la cual incorpora y tipifica los delitos informáticos al Código Penal Argentino con el objeto de regular las nuevas tecnologías como medios de comisión de delitos.

7.2.5 Comparación y diferencias de las diversas legislaciones de delitos informáticos entre los países estudiados.

Tabla 1. Similitudes y diferencias en las leyes de Nicaragua, Costa Rica, Chile y Argentina.

Comparación y diferencias de las diversas legislaciones de delitos informáticos entre los países estudiados.			
País	**Legislación**	**Similitudes**	**Diferencias**
Nicaragua	• Constitución política. • Ley No. 641. código Penal. • Ley especial de ciberdelitos. Ley N°. 1042	Tienen naturaleza transfronteriza de muchos delitos informáticos, las leyes podrían incluir disposiciones para la cooperación internacional en la investigación y	Es el país más reciente a nivel centroamericano y latinoamericano de incorporar una ley dedicada y especial a los delitos informáticos.

		persecución de estos delitos.	
Costa Rica	• Constitución política. • Incorporación al Código Penal los delitos en materia de comunicaciones electrónicas • Ley No. 9048 de Delitos Informáticos que Reformas y modifica el Código Penal	En la actualidad, los Estados conciben la ciberdelincuencia como un fenómeno social de gran relevancia, ya que implica la violación de diversos bienes jurídicos. Este enfoque refleja la complejidad y el alcance de las actividades delictivas en el ciberespacio, abarcando desde intrusiones no autorizadas en sistemas informáticos hasta la manipulación fraudulenta de información sensible.	En 2012, surgió el Centro de Respuesta a Incidentes de Seguridad Informática (CSIRTCR), conformado por especialistas cuya responsabilidad es anticipar y gestionar situaciones de ataques y amenazas cibernéticas dirigidas a las instituciones gubernamentales. Desde el año 2017, el país ha implementado una Estrategia Nacional de Ciberseguridad, la cual ha establecido las directrices fundamentales para abordar las cuestiones relacionadas con la seguridad en el ámbito digital. Este documento, al destacar principalmente los desafíos a superar y las áreas que requieren fortalecimiento, ha trazado el rumbo a seguir en el ámbito de la ciberseguridad en la nación.

			Con la Ley No. 8968 de 2011, conocida como la "Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales", Costa Rica ha emergido como uno de los países líderes en la región centroamericana en lo que respecta a la salvaguarda y manejo de la información personal de sus ciudadanos.
Chile	• Constitución de la republica • Ley núm. 21.459 establece normas sobre delitos informáticos, deroga la ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al convenio de Budapest	En Chile, dos entidades clave en la lucha contra el cibercrimen son la Brigada Investigadora de Cibercrimen, que opera bajo la Policía de Investigaciones, y el Departamento de Organizaciones Criminales, que está bajo la jurisdicción de Carabineros. Ambas instituciones, Carabineros e Investigaciones, están conectadas al Gobierno central a través del	La "cibervigilancia" y su equivalente en términos de "actividades de vigilancia" carecen de definiciones específicas en las normativas chilena y argentina, lo que crea un vacío conceptual en ambas jurisdicciones. También existe falta de definición en comparación con las legislaciones de Nicaragua y Costa Rica.

		Ministerio del Interior y Seguridad Pública.	
Argentina	• Constitución de la Nación Argentina • Ley Nacional N° 26.388 de Delitos Informáticos incorporada al Código Penal Argentino	En términos de la formulación de políticas públicas relacionadas con la ciberseguridad, hay una diferencia importante entre Argentina y Chile. A diferencia de Argentina, Chile ha iniciado formalmente el proceso de desarrollo de una Política Nacional de Ciberseguridad. En este contexto, diversos organismos participan en la identificación y planificación, incluyendo el Departamento de Crimen Organizado de la División de Estudios y la División Informática, ambas adscritas al Ministerio del Interior. Además, se cuenta con la colaboración de la Subsecretaría de Defensa del Ministerio de Defensa, los	Argentina cuenta con divisiones especializadas en delitos tecnológicos dentro de la Policía Federal, que tiene jurisdicción nacional, y la Policía Metropolitana, con jurisdicción en la Ciudad Autónoma de Buenos Aires. Además, en el ámbito del Ministerio Público Fiscal, se encuentra la Unidad Fiscal Especializada en Cibercrimen, mientras que en la Ciudad Autónoma de Buenos Aires opera la Fiscalía Especializada en Delitos Informáticos.

		Ministerios de Transporte y Telecomunicaciones, Economía, Fomento y Turismo, Relaciones Exteriores y Secretaría General de la Presidencia. También participan la Universidad de Chile, el Instituto Nacional de Normalización, el Ministerio Público y el Poder Judicial.	

VIII. CONCLUSIONES

Con la instauración de la globalización nació la tecnología, por lo que se produjeron nuevas formas de interacción entre las personas; Esto a su vez tiene consecuencias tanto positivas como negativas para la sociedad. Dentro de los cambios positivos se puede ver la introducción de componentes que facilitan la vida diaria, entre ellos: acceso a sistemas bancarios a través de aplicaciones móviles, compras internacionales a través del sitio web y transmisión de información en tiempo presente.

Con eso viene la evolución de la economía global, ya que la tecnología se ha convertido en un factor que complementa la forma en que la industria comercializa varios productos. En términos de cambios negativos, han surgido nuevas formas de corrupción y tácticas criminales debido al gran volumen de procesamiento y transferencia de datos que pertenecen al dominio privado de las personas y que son fácilmente violables.

Los ciberdelincuentes buscan explotar la información que las personas procesan a través de redes informáticas y explotar la falta de atención y conocimiento de las personas en su beneficio. Por lo tanto, se puede decir que los delitos informáticos están indisolublemente ligados al desarrollo de la tecnología.

En comparación con el derecho consuetudinario, la informática tiene características especiales que especifican sus leyes aplicables; Es necesario adaptar los mecanismos normativos nacionales e internacionales para buscar la aplicación y defensa efectivas de los derechos individuales. Asimismo, el cálculo tiene un elemento variable, lo que significa que cambia constantemente.

Los datos procesados en las redes de Internet son de gran valor para los delincuentes, por lo que las actividades que se desarrollan en el ciberespacio repercuten en actividades ilícitas que afectan al derecho penal, por lo que necesitan reaccionar y adaptarse para poder regular, prevenir y sancionar las conductas que se desarrollan en el internet.

La tipificación de los delitos informáticos hace efectiva la ejecución de la pena, porque en derecho penal el juez no puede basarse en el análisis de similitud para aplicarla y prohíbe el uso de la tipificación. Los actos legislativos están llamados a prestar atención a las definiciones de los nuevos tipos de delitos a cometer, así como qué disposiciones deben dictarse para adecuar la creación de información y así lograr sus fines. norma jurídica. propiedad, sancionar las actividades ilícitas y prevenir las actividades delictivas.

Con la finalidad de lograr una legislación uniforme sobre ciberdelincuencia, el Consejo de Europa certifico en 2001 el Convenio de Budapest, que entró en vigor en 2004. Este convenio fue el primer convenio internacional en esta materia que establecieron expertos a nivel internacional y acuerdan unir fuerzas para centralizar la información recibida durante la investigación y contar con mecanismos apropiados para regular y prevenir las diversas formas de ciberdelincuencia que ocurren en todo el mundo.

En la actualidad, Nicaragua está en crecimiento en la materia legal de los ciberdelitos, incluso cuenta con la más reciente ley, donde se adoptan diferentes crímenes ejercidos con las tecnologías de información y comunicación y se dirige a ser uno de los países en América latina que contemple firmemente esta modalidad criminal.

IX. RECOMENDACIONES

- Se recomiendan impulsar campañas de concientización sobre este tipo de delitos informáticos para que el público tome conciencia de estos ataques cibernéticos y se comunique con las autoridades pertinentes para presentar una denuncia formal.
- También se recomienda establecer unidades especializadas en delitos informáticos dentro del Ministerio de Relaciones Exteriores, el Poder Judicial y la Policía Nacional.
- Requerir capacitaciones de organizaciones centroamericanas con experiencia en la lucha contra el crimen informático para transferir este conocimiento a los funcionarios gubernamentales.
- Asimismo, se recomienda a las empresas que ofrecen servicios de internet que trabajen de la mano con el gobierno para que sea más fácil encontrar las direcciones IP de los piratas informáticos y así localizarlos más rápido.
- Instalar una oficina con la tecnología óptima para rastrear los delitos informáticos y haga que los agentes de la oficina controlen constantemente las anomalías informadas por los usuarios. Para hacer esto, debe tener una ventana que brinde soporte a los usuarios que creen que su sistema ha sido pirateado por una computadora.

X. BIBLIOGRAFÍA

Andrés, D. D. S. (2020). *Trabajo Final Integrador para la Obtención de la Especialidad en Medicina Legal*.

Avast, A. (2020). *Que es Ciberdelito y como puedo prevenirlo.* Avast academy.

Barahona, S. S. (2021). *Perfiles del ciberdelito: Un campo de estudio inexplorado. Revista de Derecho.*

Barrios, W. (2021). *Cibercrimen y delitos informáticos.*

Biblioteca del Congreso Nacional (BCN) (1993). *Historia de la Ley 19.223*.

Blasco, J., Pérez, J. (2007). *Metodologías de investigación en las ciencias de la actividad física y el deporte: ampliando horizontes.* España. Editorial Club Universitario.

Bonilla, P. (2019). *El espectro actual de los delitos informáticos*.

CEPAL. (2014). *La seguridad cibernética en América Latina y el Caribe: Un esfuerzo multilateral*. https://www.cepal.org/sites/default/files/events/files/presentation_comtelca.pdf

Chavarría Pérez, E. de la C., Jirón Vargas, M. A., & Miranda González, F. A. (2016). *La ciberdelincuencia y su regulación jurídica en Centroamérica con énfasis en Costa Rica, El Salvador y Nicaragua* http://riul.unanleon.edu.ni:8080/jspui/handle/123456789/5316

Desayes, J. (2022). *Ciberseguridad: Importancia de una estrategia centroamericana homologada para contrarrestar la ciberdelincuencia como una amenaza emergente.*

Diario Financiero. (2020). *Ciberdelincuencia en Chile: Un traje a la medida de los infractores | Diario Financiero*.

https://www.df.cl/opinion/columnistas/ciberdelincuencia-en-chile-un-traje-a-la-medida-de-los-infractores

El 19 Digital. (2020). *Conozca más sobre la Iniciativa de Ley Especial de Ciberdelitos*. El 19 Digital. http://www.el19digital.com/articulos/ver/titulo:107781-conozca-mas-sobre-la-iniciativa-de-ley-especial-de-ciberdelitos

Errius (2018). *CIBERCRIMEN Y DELITOS INFORMÁTICOS: Los nuevos tipos penales en la era de internet*. https://www.pensamientopenal.com.ar/system/files/2018/09/doctrina46963.pdf

Espinoza. (2018). *Policía alerta ante Delitos Cibernéticos*. https://www.policia.gob.ni/?p=16943

Ganon, V. (2017). *Internet la nueva era del delito, Ciberdelito, ciberterrorismo, Legislación y ciberseguridad.*

Gercke, M. (2014). *Comprensión Ciberdelitos: Fenómenos, Dificultades y repuestas Jurídicas.*

Jijena, R. (2019). *La criminalidad informática en Chile. Análisis de la Ley 19.223*. Ponencias del VI Congreso Iberoamericano de Derecho e Informática.

Kranenbarg, M. (2018). *Cyber-offenders versus traditional offenders*. An empirical comparison.

Linde, A., & Aebi, M. (2021). *¿Realmente theft quiere decir hurto? Y otras equivalencias dudosas entre las definiciones legales y criminológicas de las infracciones: Consecuencias para el estudio de la delincuencia*. Revista Española de Investigación Criminológica.

Muñiz, A. (2001). *La informática y sus desafíos para el derecho: el derecho informático como nueva rama de estudio y sus instituciones.* Memoria de Prueba, Universidad Adolfo Ibáñez.

Pino, S. A. (2016). *Delitos Informáticos. Generalidades*. Ecuador.

Quevedo, J. (2017). *Investigación y prueba del Ciberdelitos*. https://www.tdx.cat/bitstream/handle/10803/665611/JQG_TESIS.pdf?sequence=1&isAllowed=y

Quezada, M. (2021). *Análisis jurídico de la ley 1042: "Ley especial de Ciberdelitos"*.

Rodríguez, F. J. (2021). *Inteligencia estratégica en redes*. https://doi.org/10.35537/10915/130245

Sain, G. (2015) *Evolución histórica de los delitos informáticos*. Revista Pensamiento Penal

Sain, G. (2018). *Ciber Crimen y delitos informáticos. En G. Sain, Ciber Crimen y delitos informáticos*. Erreius Buenos Aires Argentina.

Sieber, U. (1998) *El problema: tipos comunes de delitos informáticos. En Aspectos legales de los delitos informáticos en la sociedad de la información*. Bruselas, Informe de la Comisión Europea

Tancara Q, C. (1993). *La investigación documental.* Temas Sociales, 17, 91-106.

Toledo, I. N., & Cruz, L. V. (2020). *Herramientas del Convenio de Budapest sobre ciberdelincuencia, y su adecuación a la legislación nacional.*

XI. ANEXOS

11.1 Anexo 1. Legislación sobre delitos informativos en Nicaragua.

LEY ESPECIAL DE CIBERDELITOS

LEY N°. 1042, aprobada el 27 de octubre de 2020

Publicada en La Gaceta, Diario Oficial N°. 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 N°. 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
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.

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.

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.

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.

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 trescientos cincuenta días multa.

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 realizado 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.

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.

11.2 Anexo 2. Legislación sobre delitos informativos en Costa Rica

EXPEDIENTE Nº 17.613: REFORMA A VARIOS ARTÍCULOS DEL CÓDIGO PENAL Y ADICIÓN DE UNA NUEVA

SECCIÓN VIII DENOMINADA "DELITOS INFORMÁTICOS y CONEXOS" AL TITULO VII DEL CÓDIGO PENAL
(TEXTO ACTUALIZADO AL 26 DE AGOSTO DE 2010)
LA ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA
DECRETA:
REFORMA A VARIOS ARTÍCULOS DEL CÓDIGO PENAL Y ADICIÓN DE UNA NUEVA SECCIÓN VIII DENOMINADA "DELITOS INFORMÁTICOS y CONEXOS" AL TITULO VII DEL CÓDIGO PENAL

ARTÍCULO 1.-
Refórmense los artículos 167, 196, 196 bis, 209, 214, 217 bis, 229 bis Y 288 del Código Penal, Ley N.º 4573, del 4 de mayo de 1970 y sus reformas, y se lean como sigue:

Artículo 167.- Corrupción
Será sancionado con pena de prisión de tres a ocho años, quien mantenga o promueva la corrupción de una persona menor de edad o incapaz, con fines eróticos, pornográficos u obscenos, en exhibiciones o espectáculos públicos o privados, aunque la persona menor de edad o incapaz lo consienta.
La pena será de cuatro a diez años de prisión si el actor utilizando las redes sociales o cualquier otro medio informático o telemático, u otro medio de comunicación busca encuentros de carácter sexual para sí o para otro, o para grupos, con una persona menor de edad o incapaz, o utiliza a estas personas para promover la corrupción, o los obliga a realizar actos sexuales perversos, prematuros o excesivos, aunque la víctima consienta participar en ellos o verlos ejecutar.

Artículo 196.- Violación de correspondencia o comunicaciones
Será reprimido con pena de prisión de tres a seis años quien, con peligro o daño para la intimidad o privacidad de un tercero, y sin su autorización se apodere, accese, modifique, altere, suprima, intervenga, intercepte, utilice, abra, difunda o desvíe de su destino documentos o comunicaciones dirigidas a otra persona.
La pena será de cuatro a ocho años de prisión si las conductas descritas son realizadas por:
a) Las personas encargadas de la recolección, entrega o salvaguarda de los documentos o comunicaciones; o
b) Las personas encargadas de administrar o dar soporte al sistema o red informática o telemática, o que en razón de sus funciones tengan acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.

Artículo 196 Bis.- Violación de datos personales

Será sancionado con pena de prisión de tres a seis años quien en beneficio propio o de un tercero, y con peligro o daño para la intimidad o privacidad y sin la autorización del titular de los datos, se apodere, modifique, interfiera, acceda, copie, transmita, publique, difunda, recopile, inutilice, intercepte, retenga, venda, compre, desvíe para un fin distinto para el que

fueron recolectados o dé un tratamiento no autorizado a las imágenes o datos de una persona física o jurídica almacenados en sistemas o redes informáticas o telemáticas, o en contenedores electrónicos, ópticos o magnéticos.
La pena será de cuatro a ocho años de prisión, cuando las conductas descritas en esta norma:
a) Sean realizadas por personas encargadas de administrar o dar soporte al sistema o red informática o telemática, o que en razón de sus funciones tengan acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.
b) Cuando los datos sean de carácter público o estén contenidas en bases de datos públicas.
c) Si la información vulnerada corresponde a un menor de edad o incapaz.
d) Cuando las conductas afecten datos que revelen la ideología, religión, creencias, salud, origen racial, preferencia o vida sexual de una persona.

Artículo 209.- **Hurto agravado**

Se aplicará prisión de uno a nueve años, si el valor de lo sustraído no excede de cinco veces el salario base, y de cinco a diez años, si fuere mayor de esa suma, en los siguientes casos:

a) Cuando el hurto fuere sobre cabezas de ganado mayor o menor, aves de corral, productos o elementos que se encuentren en uso para la explotación agropecuaria.
b) Si fuera cometido aprovechando las facilidades provenientes de un estrago, de una conmoción pública o de un infortunio particular del damnificado;
c) Si se hiciere uso de ganzúa, llave falsa u otro instrumento semejante, o de la llave verdadera que hubiere sido sustraída, hallada o retenida, claves de acceso, tarjetas magnéticas o dispositivos electrónicos.
d) Si fuere de equipaje de viajeros, en cualquier clase de vehículos o en los estacionamientos o terminales de las empresas de transportes;
e) Si fuere de vehículos dejados en la vía pública o en lugares de acceso público;
f) Si fuere de cosas de valor científico, artístico, cultural, de seguridad o religioso, cuando por el lugar en que se encuentren estén destinadas al servicio, a la utilidad o a la reverencia de un número indeterminado de personas, o libradas a la confianza pública; y
g) Si fuere cometido por dos o más personas.

Artículo 214.- **Extorsión**
Será reprimido con pena de prisión de cuatro a ocho años, al que para procurar un lucro obligare a otro con intimidación o con amenazas graves a tomar una disposición patrimonial perjudicial para sí mismo o para un tercero.

La pena será de cinco a diez años de prisión cuando la conducta se realice valiéndose de cualquier manipulación informática, telemática, electrónica o tecnológica.

Artículo 217 Bis. - Fraude informático

Se impondrá prisión de tres a seis años a quien, en perjuicio de una persona física o jurídica, manipule o influya en el ingreso, en el procesamiento o en el resultado de los datos de un sistema automatizado de información, ya sea mediante el uso de datos falsos o incompletos, uso indebido de datos, programación, valiéndose de alguna operación informática, o artificio tecnológico, o por cualquier otra acción que incida en el procesamiento de los datos del sistema o que dé como resultado información falsa, incompleta o fraudulenta, con la cual procure u obtenga un beneficio patrimonial o indebido para sí o para otro.
La pena será de cinco a diez años de prisión si las conductas son cometidas contra sistemas de información públicos, sistema de información bancarios, de entidades financieras o cuando el autor es un empleado encargado de administrar o dar soporte al sistema o red informática o telemática, o que en razón de sus funciones tengan acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.

Artículo 229 Bis. - Daño informático

Se impondrá pena de prisión de uno a tres años, al que, sin autorización del titular, o excediendo la que se le hubiere concedido y en perjuicio de un tercero, suprima, modifique o destruya la información contenida en un sistema o red informática o telemática, o en contenedores electrónicos, ópticos o magnéticos.
La pena será de tres a seis años de prisión, si la información suprimida, modificada, destruida es insustituible o irrecuperable.

Artículo 288.- Espionaje

Será reprimido con prisión de cuatro a ocho años, el que procurare u obtuviere indebidamente informaciones secretas políticas o de los cuerpos de policía nacionales, o de seguridad concernientes a los medios de defensa o a las relaciones exteriores de la Nación, o afecte la lucha contra el narcotráfico o el crimen organizado.

La pena será de cinco a diez años de prisión, cuando la conducta se realice mediante manipulación informática, programas informáticos maliciosos o por el uso de tecnologías de la información y la comunicación.

ARTÍCULO 2.-

Adiciónese un nuevo inciso 6) al artículo 229 y un artículo 229 ter al Código Penal, Ley N.º 4573, del 4 de mayo de 1970 y sus reformas, los cuales se leerán como sigue:

ARTÍCULO 229.- Daño agravado
Se impondrá prisión de seis meses a cuatro años:

6) Cuando el daño recayere sobre redes, sistemas o equipos informáticos, telemáticas o electrónicos, o sus componentes físicos, lógicos o periféricos.

ARTÍCULO 229 Ter. - Sabotaje informático

Se impondrá pena de prisión de tres a seis años, al que, en provecho propio o de un tercero, destruya, altere, entorpezca o inutilice la información contenida en una base de datos, o impida, altere, obstaculice o modifique sin autorización, el funcionamiento de un sistema de tratamiento de información, sus partes o componentes físicos o lógicos, o un sistema informático.

La pena será de cuatro a ocho años de prisión, cuando:

a) Como consecuencia de la conducta del autor sobreviniere peligro colectivo o daño social.
b) La conducta se realizare por parte de un empleado encargado de administrar o dar soporte al sistema o red informática o telemática, o que en razón de sus funciones tengan acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.
c) El sistema informático sea de carácter público o la información está contenida en bases de datos públicas.
d) Sin estar facultado, emplee medios tecnológicos que impidan a personas autorizadas el acceso lícito de los sistemas o redes de telecomunicaciones.

ARTÍCULO 3.-

Modifíquese la Sección VIII del Título VII del Código Penal, Ley N.º 4573, del 4 de mayo de 1970 y sus reformas y se corra la numeración de los artículos subsiguientes, para que se lea como sigue:

Sección VIII
DELITOS INFORMÁTICOS y CONEXOS
Artículo 230.- Suplantación de identidad

Será sancionado con pena de prisión de tres a seis años, quien suplante la identidad de una persona en cualquier red social, sitio de internet, medio electrónico o tecnológico de información. En la misma pena incurrirá quien utilizando una identidad falsa o inexistente cause perjuicio a un tercero.

La pena será de cuatro a ocho años de prisión si con las conductas anteriores se causa un perjuicio a una persona menor de edad o incapaz.”

Artículo 231.- **Espionaje informático**

Se impondrá prisión de tres a seis años al que, sin autorización del titular o responsable, valiéndose de cualquier manipulación informática o tecnológica, se apodere, transmita, copie, modifique, destruya, utilice, bloquee o recicle, información de valor para el tráfico económico de la industria y el comercio.

Artículo 232.- **Instalación o propagación de Programas informáticos maliciosos**

Será sancionado con prisión de uno a seis años, quien, sin autorización, y por cualquier medio, instale programas informáticos maliciosos en un sistema o red informática o telemática, o en los contenedores electrónicos, ópticos o magnéticos.
La misma pena se impondrá en los siguientes casos:

a) A quien induzca a error a una persona para que instale un programa informático malicioso en un sistema o red informática o telemática, o en los contenedores electrónicos, ópticos o magnéticos, sin la debida autorización.
b) A quien, sin autorización instale programas o aplicaciones informáticas dañinas en sitios de Internet legítimos, con el fin de convertidos en medios idóneos para propagar programas informáticos maliciosos, conocidos como Sitios de Internet Atacantes.
c) A quien, para propagar programas informáticos maliciosos, invite a otras personas a descargar archivos o a visitar sitios de internet que permita la instalación de programas informáticos maliciosos.
d) A quien distribuya programas informáticos diseñados para la creación de programas informáticos maliciosos.
e) A quien ofrezca, contrate o brinde servicios de denegación de servicios, envío de comunicaciones masivas no solicitadas, o propagación de programas informáticos maliciosos.

La pena será de tres a nueve años de prisión cuando el programa informático malicioso:

i. Afecte a una entidad bancaria, financiera, cooperativa de ahorro y crédito, asociación solidarista o ente estatal.
ii. Afecte el funcionamiento de servicios públicos.
iii. Obtenga el control a distancia de un sistema o de una red informática, para formar parte de una red de ordenadores zombi.
iv. Esté diseñado para realizar acciones dirigidas a procurar un beneficio patrimonial para sí o para un tercero.
v. Afecte sistemas informáticos de la salud y la afectación de los mismos pueda poner en peligro la salud o vida de las personas.
vi. Tenga la capacidad de reproducirse sin la necesidad de intervención adicional por parte del usuario legítimo del sistema informático.

Artículo 233.- **Suplantación de páginas electrónicas**

Se impondrá pena de prisión de uno a tres años, a quien, en perjuicio de un tercero, suplante sitios legítimos de la red de Internet.

La pena será de tres a seis años de prisión cuando como consecuencia de la suplantación del sitio legítimo de Internet, y mediante engaño o haciendo incurrir en error, capture información confidencial de una persona física o jurídica para beneficio propio o de un tercero.

Artículo 234.- **Facilitación del delito informático**

Se impondrá pena de prisión de uno a cuatro años a quien facilite los medios para la consecución de un delito efectuado mediante un sistema o red informática o telemática, o los contenedores electrónicos, ópticos o magnéticos

Artículo 235.- **Narcotráfico y crimen organizado**

La pena se duplicará cuando cualquiera de los delitos cometidos por medio un sistema o red informática o telemática, o los contenedores electrónicos, ópticos o magnéticos afecte la lucha contra el narcotráfico o el crimen organizado.

Artículo 236.- **Difusión de Información Falsa**
Será sancionado con pena de tres a seis años de prisión quien, a través de medios electrónicos, informáticos, o mediante un sistema de telecomunicaciones propague o difunda noticias, o hechos falsos capaces de distorsionar o causar perjuicio a la seguridad y estabilidad del sistema financiero o de sus usuarios.

ARTÍCULO 4.-

Modifíquese el artículo 9 de la Ley sobre Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones y sus reformas, N.º 7425 de 09 de agosto de 1994 y se lea como sigue:

Artículo 9.- **Autorización de intervenciones.**

Dentro de los procedimientos de una investigación policial o jurisdiccional, los tribunales de justicia podrán autorizar la intervención de comunicaciones orales, escritas o de otro tipo, incluso las telecomunicaciones fijas, móviles, inalámbricas y digitales, cuando involucre el esclarecimiento de los siguientes delitos: delitos informáticos o cometidos mediante la utilización de medios informáticos, electrónicos, telemáticos, ópticos o magnéticos, secuestro extorsivo, corrupción agravada, proxenetismo agravado, fabricación o producción de pornografía, tráfico de personas y tráfico de personas para comercializar sus órganos; homicidio calificado; genocidio, terrorismo y los delitos previstos en la Ley sobre

estupefacientes, sustancias psicotrópicas, drogas de uso no autorizado, legitimación de capitales y actividades conexas, N.° 8204, del 26 de diciembre del 2001.

En los mismos casos, dichos tribunales podrán autorizar la intervención de las comunicaciones entre los presentes, excepto lo dispuesto en el segundo párrafo del artículo 26 de la presente Ley; cuando se produzcan dentro de domicilios y recintos privados, la intervención solo podrá autorizarse si existen indicios suficientes de que se lleva a cabo una actividad delictiva."

Rige a partir de su publicación.

11.3 Anexo 3. Legislación sobre delitos informativos en Chile.

LEY NÚM. 21.459

ESTABLECE NORMAS SOBRE DELITOS INFORMÁTICOS, DEROGA LA LEY N° 19.223 Y MODIFICA OTROS CUERPOS LEGALES CON EL OBJETO DE ADECUARLOS AL CONVENIO DE BUDAPEST

Teniendo presente que el H. Congreso Nacional ha dado su aprobación al siguiente

Proyecto de ley:

"TÍTULO I

DE LOS DELITOS INFORMÁTICOS Y SUS SANCIONES

Artículo 1°. - Ataque a la integridad de un sistema informático. El que obstaculice o impida el normal funcionamiento, total o parcial, de un sistema informático, a través de la introducción, transmisión, daño, deterioro, alteración o supresión de los datos informáticos, será castigado con la pena de presidio menor en sus grados medio a máximo.

Artículo 2°. - Acceso ilícito. El que, sin autorización o excediendo la autorización que posea y superando barreras técnicas o medidas tecnológicas de seguridad, acceda a un sistema informático será castigado con la pena de presidio menor en su grado mínimo o multa de once a veinte unidades tributarias mensuales.

Si el acceso fuere realizado con el ánimo de apoderarse o usar la información contenida en el sistema informático, se aplicará la pena de presidio menor en sus grados mínimo a medio. Igual pena se aplicará a quien divulgue la información a la cual se accedió de manera ilícita, si no fuese obtenida por éste.

En caso de ser una misma persona la que hubiere obtenido y divulgado la información, se aplicará la pena de presidio menor en sus grados medio a máximo.

Artículo 3°. - Interceptación ilícita. El que indebidamente intercepte, interrumpa o interfiera, por medios técnicos, la transmisión no pública de información en un sistema informático o entre dos o más de aquellos, será castigado con la pena de presidio menor en su grado medio.

El que, sin contar con la debida autorización, capte, por medios técnicos, datos contenidos en sistemas informáticos a través de las emisiones electromagnéticas provenientes de éstos, será castigado con la pena de presidio menor en sus grados medio a máximo.

Artículo 4°. - Ataque a la integridad de los datos informáticos. El que indebidamente altere, dañe o suprima datos informáticos, será castigado con presidio menor en su grado medio, siempre que con ello se cause un daño grave al titular de estos mismos.

Artículo 5°. - Falsificación informática. El que indebidamente introduzca, altere, dañe o suprima datos informáticos con la intención de que sean tomados como auténticos o utilizados para generar documentos auténticos, será sancionado con la pena de presidio menor en sus grados medio a máximo.

Cuando la conducta descrita en el inciso anterior sea cometida por empleado público, abusando de su oficio, será castigado con la pena de presidio menor en su grado máximo a presidio mayor en su grado mínimo.

Artículo 6°. - Receptación de datos informáticos. El que conociendo su origen o no pudiendo menos que conocerlo comercialice, transfiera o almacene con el mismo objeto u otro fin ilícito, a cualquier título, datos informáticos, provenientes de la realización de las conductas descritas en los artículos 2°, 3° y 5°, sufrirá la pena asignada a los respectivos delitos, rebajada en un grado.

Artículo 7°. - Fraude informático. El que, causando perjuicio a otro, con la finalidad de obtener un beneficio económico para sí o para un tercero, manipule un sistema informático, mediante la introducción, alteración, daño o supresión de datos informáticos o a través de cualquier interferencia en el funcionamiento de un sistema informático, será penado:

1) Con presidio menor en sus grados medio a máximo y multa de once a quince unidades tributarias mensuales, si el valor del perjuicio excediera de cuarenta unidades tributarias mensuales.

2) Con presidio menor en su grado medio y multa de seis a diez unidades tributarias mensuales, si el valor del perjuicio excediere de cuatro unidades tributarias mensuales y no pasare de cuarenta unidades tributarias mensuales.

3) Con presidio menor en su grado mínimo y multa de cinco a diez unidades tributarias mensuales, si el valor del perjuicio no excediere de cuatro unidades tributarias mensuales.

Si el valor del perjuicio excediere de cuatrocientas unidades tributarias mensuales, se aplicará la pena de presidio menor en su grado máximo y multa de veintiuna a treinta unidades tributarias mensuales.

Para los efectos de este artículo se considerará también autor al que, conociendo o no pudiendo menos que conocer la ilicitud de la conducta descrita en el inciso primero, facilita los medios con que se comete el delito.

Artículo 8º.- Abuso de los dispositivos. El que para la perpetración de los delitos previstos en los artículos 1° a 4° de esta ley o de las conductas señaladas en el artículo 7° de la ley N° 20.009, entregare u obtuviere para su utilización, importare, difundiera o realizare otra forma de puesta a disposición uno o más dispositivos, programas computacionales, contraseñas, códigos de seguridad o de acceso u otros datos similares, creados o adaptados principalmente para la perpetración de dichos delitos, será sancionado con la pena de presidio menor en su grado mínimo y multa de cinco a diez unidades tributarias mensuales.

Artículo 9°. - Circunstancia atenuante especial. Será circunstancia atenuante especial de responsabilidad penal, y permitirá rebajar la pena hasta en un grado, la cooperación eficaz que conduzca al esclarecimiento de hechos investigados que sean constitutivos de alguno de los delitos previstos en esta ley o permita la identificación de sus responsables; o sirva para prevenir o impedir la perpetración o consumación de otros delitos de igual o mayor gravedad contemplados en esta ley.

Se entiende por cooperación eficaz el suministro de datos o informaciones precisas, verídicas y comprobables, que contribuyan necesariamente a los fines señalados en el inciso anterior.

El Ministerio Público deberá expresar, en la formalización de la investigación o en su escrito de acusación, si la cooperación prestada por el imputado ha sido eficaz a los fines señalados en el inciso primero.

La reducción de pena se determinará con posterioridad a la individualización de la sanción penal según las circunstancias atenuantes o agravantes comunes que concurran; o de su compensación, de acuerdo con las reglas generales.

Artículo 10.- Circunstancias agravantes. Constituyen circunstancias agravantes de los delitos de que trata esta ley:

1) Cometer el delito abusando de una posición de confianza en la administración del sistema informático o custodio de los datos informáticos contenidos en él, en razón del ejercicio de un cargo o función.

2) Cometer el delito abusando de la vulnerabilidad, confianza o desconocimiento de niños, niñas, adolescentes o adultos mayores.

Asimismo, si como resultado de la comisión de las conductas contempladas en este Título, se afectase o interrumpiese la provisión o prestación de servicios de utilidad pública, tales como electricidad, gas, agua, transporte, telecomunicaciones o financieros, o el normal desenvolvimiento de los procesos electorales regulados en la ley Nº 18.700, orgánica constitucional sobre votaciones populares y escrutinios, la pena correspondiente se aumentará en un grado.

TÍTULO II

DEL PROCEDIMIENTO

Artículo 11.- Sin perjuicio de las reglas contenidas en el Código Procesal Penal, las investigaciones a que dieren lugar los delitos previstos en esta ley también podrán iniciarse por querella del ministro del Interior y Seguridad Pública, de los delegados presidenciales regionales y de los delegados presidenciales provinciales, cuando las conductas señaladas en esta ley interrumpieren el normal funcionamiento de un servicio de utilidad pública.

Artículo 12.- Cuando la investigación de los delitos contemplados en los artículos 1°, 2°, 3°, 4°, 5° y 7° de esta ley lo hiciere imprescindible y existieren fundadas sospechas basadas en hechos determinados, de que una persona hubiere cometido o participado en la preparación o comisión de algunos de los delitos contemplados en los preceptos precedentemente señalados, el juez de garantía, a petición del Ministerio Público, quien deberá presentar informe previo detallado respecto de los hechos y la posible participación, podrá ordenar la realización de las técnicas previstas y reguladas en los artículos 222 a 226 del Código Procesal Penal, conforme lo disponen dichas normas.

La orden que disponga la realización de estas técnicas deberá indicar circunstanciadamente el nombre real o alias y dirección física o electrónica del afectado por la medida y señalar el tipo y la duración de la misma. El juez podrá prorrogar la duración de esta orden, para lo cual deberá examinar cada vez la concurrencia de los requisitos previstos en el inciso precedente.

De igual forma, cumpliéndose los requisitos establecidos en el inciso anterior, el juez de garantía, a petición del Ministerio Público, podrá ordenar a funcionarios policiales actuar bajo identidad supuesta en comunicaciones mantenidas en canales cerrados de comunicación, con el fin de esclarecer los hechos tipificados como delitos en esta ley, establecer la identidad y participación de personas determinadas en la comisión de los mismos, impedirlos o comprobarlos. El referido agente encubierto en línea podrá intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido, pudiendo obtener también imágenes y grabaciones de las referidas comunicaciones. No obstará a la

consumación de los delitos que se pesquisen el hecho de que hayan participado en su investigación agentes encubiertos. El agente encubierto en sus actuaciones estará exento de responsabilidad criminal por aquellos delitos en que deba incurrir o que no haya podido impedir, siempre que sean consecuencia necesaria del desarrollo de la investigación y guarden la debida proporcionalidad con la finalidad de la misma.

Artículo 13.- Sin perjuicio de las reglas generales, caerán especialmente en comiso los instrumentos de los delitos penados en esta ley, los efectos que de ellos provengan y las utilidades que hubieren originado, cualquiera que sea su naturaleza jurídica.

Cuando por cualquier circunstancia no sea posible decomisar estas especies, se podrá aplicar el comiso a una suma de dinero equivalente a su valor, respecto de los responsables del delito. Si por la naturaleza de la información contenida en las especies, éstas no pueden ser enajenadas a terceros, se podrá ordenar la destrucción total o parcial de los instrumentos del delito y los efectos que de ellos provengan.

Artículo 14.- Sin perjuicio de las reglas generales, los antecedentes de investigación que se encuentren en formato electrónico y estén contenidos en documentos electrónicos o sistemas informáticos o que correspondan a datos informáticos, serán tratados en conformidad a los estándares definidos para su preservación o custodia en el procedimiento respectivo, de acuerdo a las instrucciones generales que al efecto dicte el fiscal nacional.

TÍTULO III

DISPOSICIONES FINALES

Artículo 15.- Para efectos de esta ley, se entenderá por:

a) Datos informáticos: Toda representación de hechos, información o conceptos expresados en cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función.

b) Sistema informático: Todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa.

c) Prestadores de servicios: Toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar a través de un sistema informático y cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios del mismo.

Artículo 16.- Autorización e Investigación Académica. Para efectos de lo previsto en el artículo 2° se entenderá que cuenta con autorización para el acceso a un sistema informático, el que en el marco de investigaciones de vulnerabilidad o para mejorar la seguridad informática, acceda a un sistema informático mediando la autorización expresa del titular del mismo.

Artículo 17.- Sin perjuicio de lo dispuesto en el artículo primero transitorio de esta ley, derogase la ley N° 19.223. Toda referencia legal o reglamentaria a dicho cuerpo legal debe entenderse hecha a esta ley.

Artículo 18.- Modificase el Código Procesal Penal en el siguiente sentido:

1) agregase el siguiente artículo 218 bis, nuevo:

"Artículo 218 bis. - Preservación provisoria de datos informáticos. El Ministerio Público con ocasión de una investigación penal podrá requerir, a cualquier proveedor de servicio, la conservación o protección de datos informáticos o informaciones concretas incluidas en un sistema informático, que se encuentren a su disposición hasta que se obtenga la respectiva autorización judicial para su entrega. Los datos se conservarán durante un período de 90 días, prorrogable una sola vez, hasta que se autorice la entrega o se cumplan 180 días. La empresa requerida estará obligada a prestar su colaboración y guardar secreto del desarrollo de esta diligencia.".

2) Suprímase, en el inciso primero del artículo 223, la expresión "telefónica".

3) Reemplazase, en el artículo 225, la voz "telecomunicaciones" por "comunicaciones".

Artículo 19.- Intercalase, en el literal a) del inciso primero del artículo 27 de la ley N° 19.913, que crea la Unidad de Análisis Financiero y modifica diversas disposiciones en materia de lavado y blanqueo de activos, entre las expresiones "orgánica constitucional del Banco Central de Chile;" y "en el párrafo tercero del número 4° del artículo 97 del Código Tributario", la frase "en el Título I de la ley que sanciona los delitos informáticos;".

Artículo 20.- Agregase, en el inciso primero del artículo 36 B de la ley N° 18.168, General de Telecomunicaciones, la siguiente letra f), nueva:

"f) Los que vulneren el deber de reserva o secreto previsto en los artículos 218 bis, 219 y 222 del Código Procesal Penal, mediante el acceso, almacenamiento o difusión de los antecedentes o la información señalados en dichas normas, serán sancionados con la pena de presidio menor en su grado máximo.".

Artículo 21.- Modificase la ley N° 20.393, que establece la responsabilidad penal de las personas jurídicas en los delitos de lavado de activos, financiamiento del terrorismo y delitos de cohecho que indica, en el siguiente sentido:

1) intercálese, en el inciso primero del artículo 1, a continuación de la expresión "Nº 18.314", la expresión ", en el Título I de la ley que sanciona delitos informáticos".

2)) intercálese, en el inciso primero del artículo 15, entre "Código Penal," y "y en el artículo 8°", la expresión "en el Título I de la ley que sanciona delitos informáticos".

ARTÍCULOS TRANSITORIOS

Artículo primero. - Los hechos perpetrados con anterioridad a la entrada en vigor de la presente ley, así como las penas y las demás consecuencias que correspondiere imponer por ellos, serán determinados conforme a la ley vigente en el momento de su perpetración. Si la presente ley entrare en vigor durante la perpetración del hecho se estará a lo dispuesto en ella, siempre que en la fase de perpetración posterior se realizare íntegramente la nueva descripción legal del hecho.

Si la aplicación de la presente ley resultare más favorable al imputado o acusado por un hecho perpetrado con anterioridad a su entrada en vigor, se estará a lo dispuesto en ella. Para determinar si la aplicación de esta ley resulta más favorable, se deberá tomar en consideración todas las normas en ella previstas que fueren pertinentes al juzgamiento del hecho.

Para efectos de lo dispuesto en los incisos primero y segundo precedentes, el delito se entiende perpetrado en el momento o durante el lapso en el cual se ejecuta la acción punible o se incurre en la omisión punible.

Artículo segundo. - El artículo 18 de la presente ley comenzará a regir transcurridos seis meses desde la publicación en el Diario Oficial de un reglamento dictado por el Ministerio de Transportes y Telecomunicaciones, suscrito además por el ministro del Interior y Seguridad Pública.

El reglamento señalado en el inciso anterior deberá dictarse dentro del plazo de seis meses, contado desde la publicación de la presente ley en el Diario Oficial.

Artículo tercero. - Los artículos 19 y 21 comenzarán a regir transcurridos seis meses desde la publicación de la presente ley en el Diario Oficial.".

Habiéndose cumplido con lo establecido en el Nº 1 del artículo 93 de la Constitución Política de la República y por cuanto he tenido a bien aprobarlo y sancionarlo; por tanto, promúlguese y llévese a efecto como Ley de la República.

Santiago, 9 de junio de 2022.- IZKIA SICHES PASTÉN, vicepresidenta de la República. - Marcela Ríos Tobar, ministra de Justicia y Derechos Humanos. - Manuel Monsalve Benavides, ministro del Interior y Seguridad Pública (S). - Juan Carlos Muñoz Abogabir, ministro de Transportes y Telecomunicaciones.

Lo que transcribo a Ud. para su conocimiento. - Saluda atentamente a Ud., Jaime Gajardo Falcón, Subsecretario de Justicia.

Tribunal Constitucional

Proyecto de ley que establece normas sobre delitos informáticos, deroga la ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest, correspondiente al Boletín N° 12.192-25.

La secretaria del Tribunal Constitucional, quien suscribe, certifica que el Honorable Senado de la República envió el proyecto de ley enunciado en el rubro, aprobado por el Congreso Nacional, a fin de que este Tribunal ejerciera el control de constitucionalidad respecto de sus artículos 9, inciso tercero; 12; 14; y 218 bis contenido en el numeral 1) del artículo 18 del proyecto; y por sentencia de 26 de mayo de 2022, en los autos Rol 13185-22- CPR.

Se declara:

1°. Que los artículos 9, inciso tercero, 14 y 18 del proyecto de ley que establece normas sobre delitos informáticos, deroga la Ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest, correspondiente al Boletín N° 12.192-25 son conformes con la Constitución Política.

2°. Que no se emite pronunciamiento, en examen preventivo de constitucionalidad, de las restantes disposiciones del proyecto de ley, por no versar sobre materias reguladas en Ley Orgánica Constitucional.

Santiago, 27 de mayo de 2022.- María Angélica Barriga Meza, secretaria.

11.4 Anexo 4. Legislación sobre delitos informativos en Argentina.

CODIGO PENAL
Ley 26.388 Modificación.
Sancionada: Junio 4 de 2008
Promulgada de Hecho: Junio 24 de 2008

El Senado y Cámara de Diputados de la Nación Argentina reunidos en Congreso, etc. sancionan con fuerza de Ley:

ARTICULO 1º — Incorpórense como últimos párrafos del artículo 77 del Código Penal, los siguientes: El término "documento" comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión. Los términos "firma" y "suscripción" comprenden la firma digital, la creación de una firma digital o firmar digitalmente. Los términos "instrumento privado" y "certificado" comprenden el documento digital firmado digitalmente.

ARTICULO 2º — Sustitúyase el artículo 128 del Código Penal, por el siguiente: Artículo 128: Será reprimido con prisión de seis (6) meses a cuatro (4) años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho (18) años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores. Será reprimido con prisión de cuatro (4) meses a dos (2) años el que tuviere en su poder representaciones de las descriptas en el párrafo anterior con fines inequívocos de distribución o comercialización. Será reprimido con prisión de un (1) mes a tres (3) años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce (14) años.

ARTICULO 3º — Sustitúyase el epígrafe del Capítulo III, del Título V, del Libro II del Código Penal, por el siguiente: "Violación de Secretos y de la Privacidad"

ARTICULO 4º — sustituyese el artículo 153 del Código Penal, por el siguiente: Artículo 153: Será reprimido con prisión de quince (15) días a seis (6) meses el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel 2 privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida. En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido. La pena será de prisión de un (1) mes a un (1) año, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación

electrónica. Si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá, además, inhabilitación especial por el doble del tiempo de la condena.

ARTICULO 5º — Incorpórese como artículo 153 bis del Código Penal, el siguiente: Artículo 153 bis: Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido. La pena será de un (1) mes a un (1) año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros.

ARTICULO 6º — sustituyese el artículo 155 del Código Penal, por el siguiente: Artículo 155: Será reprimido con multa de pesos un mil quinientos ($ 1.500) a pesos cien mil ($ 100.000), el que, hallándose en posesión de una correspondencia, una comunicación electrónica, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, no destinados a la publicidad, los hiciere publicar indebidamente, si el hecho causare o pudiere causar perjuicios a terceros. Está exento de responsabilidad penal el que hubiere obrado con el propósito inequívoco de proteger un interés público.

ARTICULO 7º — sustituyese el artículo 157 del Código Penal, por el siguiente: Artículo 157: Será reprimido con prisión de un (1) mes a dos (2) años e inhabilitación especial de un (1) a cuatro (4) años, el funcionario público que revelare hechos, actuaciones, documentos o datos, que por ley deben ser secretos.

ARTICULO 8º — sustituyese el artículo 157 bis del Código Penal, por el siguiente: Artículo 157 bis: Será reprimido con la pena de prisión de un (1) mes a dos (2) años el que: 1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales; 2. Ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley. 3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales. 3.Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de un (1) a cuatro (4) años.

ARTICULO 9º — incorporase como inciso 16 del artículo 173 del Código Penal, el siguiente: Inciso 16. El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos.

ARTICULO 10. — incorporase como segundo párrafo del artículo 183 del Código Penal, el siguiente: En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños.

ARTICULO 11. — sustituyese el artículo 184 del Código Penal, por el siguiente: Artículo 184: La pena será de tres (3) meses a cuatro (4) años de prisión, si mediare cualquiera de las circunstancias siguientes: 1. Ejecutar el hecho con el fin de impedir el libre ejercicio de la autoridad o en venganza de sus determinaciones; 2. Producir infección o contagio en aves u otros animales domésticos; 3. Emplear substancias venenosas o corrosivas; 4. Cometer el delito en despoblado y en banda; 5. Ejecutarlo en archivos, registros, bibliotecas, museos o en puentes, caminos, paseos u otros bienes de uso público; o en tumbas, signos conmemorativos, monumentos, estatuas, cuadros u otros objetos de arte colocados en edificios o lugares públicos; o en datos, documentos, programas o sistemas informáticos públicos; 6. Ejecutarlo en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público.

ARTICULO 12. — sustituyese el artículo 197 del Código Penal, por el siguiente: Artículo 197: Será reprimido con prisión de seis (6) meses a dos (2) años, el que interrumpiere o entorpeciere la comunicación telegráfica, telefónica o de otra naturaleza o resistiere violentamente el restablecimiento de la comunicación interrumpida.

ARTICULO 13. — sustituyese el artículo 255 del Código Penal, por el siguiente: Artículo 255: Será reprimido con prisión de un (1) mes a cuatro (4) años, el que sustrajere, alterare, ocultare, destruyere o inutilizare en todo o en parte objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario público o de otra persona en el interés del servicio público. Si el autor fuere el mismo depositario, sufrirá además inhabilitación especial por doble tiempo. Si el hecho se cometiere por imprudencia o negligencia del depositario, éste será reprimido con multa de setecientos cincuenta pesos ($ 750) a doce mil quinientos pesos ($ 12.500).

ARTICULO 14. — Derogase el artículo 78 bis y el inciso 1º del artículo 117 bis del Código Penal.

ARTICULO 15. — Comuníquese al Poder Ejecutivo.

DADA EN LA SALA DE SESIONES DEL CONGRESO ARGENTINO, EN BUENOS AIRES, A LOS CUATRO DIAS DEL MES DE JUNIO DEL AÑO DOS MIL OCHO. — REGISTRADO BAJO EL Nº 26.388 — EDUARDO A. FELLNER. — JULIO C. C. COBOS. — Enrique Hidalgo. — Juan H. Estrada.

11.5 Anexo 5. Casos en donde se aplico la Ley de Ciberdelito en Nicaragua

11.5.1 Insólito: condenaron por “ciberdelitos” a 11 años de cárcel a un campesino de Nicaragua que apenas lee y nunca usó PC ni smartphone

Santos Camilo Bellorín no usa teléfono inteligente ni computadoras, pero fue condenado a 11 años de cárcel por "ciberdelitos". (Foto cortesía)

Hasta el 6 de noviembre del año pasado, **Santos Camilo Bellorín llevaba una vida dedicada al cultivo de maíz, frijoles y café en la comunidad de Guasuyuca**, Pueblo Nuevo, a 200 kilómetros al norte de Managua. Ese día fue detenido por primera vez

El 9 de noviembre fue liberado. **Dos días después fue apresado nuevamente y esta vez acusado de como autor ciberdelitos en contra del Estado de Nicaragua.**

El juicio contra Bellorín, de 56 años, se realizó el pasado 10 de febrero y este martes fue leída su condena: 11 años de prisión. Para su familia la acusación fue una absurda sorpresa. Según Francisco Bellorín, hermano del condenado, “**Santos ni**

conoce las computadoras" y solo manejaba un teléfono celular básico, no inteligente y sin conexión a internet.

El juez Erick Ramón Laguna Averruz, del Juzgado de Distrito Penal de Juicio de Estelí, lo declarara culpable por el delito de "propagación de noticias falsas", según la Ley 1042, Ley Especial de Ciberdelitos, aprobada en octubre de 2020.

Esta ley, junto a la 1055, conocida como "Ley de Soberanía", son las más utilizadas

En la acusación, el Ministerio Público señala a Santos Camilo Bellorín de **provocar "alarma, temor y zozobra" entre la población a través del uso de las redes sociales.** Le atribuye además **destrezas "en sistemas informáticos, tecnologías de la información y comunicación en el ciberespacio, redes sociales tales como Facebook y Twitter a los que accedía a través de un dispositivo móvil o desde una de las aplicaciones a través de su cuenta personal en Twitter registrada con el perfil a nombre Santos Bellorín @Santos51".**

El perfil aludido fue creado en abril de 2009, está a nombre de Anisio Santos, tiene solo cinco seguidores y ni solo un tuit publicado.

Entre las pruebas presentadas por la Fiscalía están media docena de publicaciones de Twitter y Facebook y un supuesto retuit que Bellorín habría hecho del ciudadano Alexis Peralta Espinoza, condenado también por el mismo delito.

Entre las pruebas presentadas por la Fiscalía está este tuit que Bellorín habría retuiteado.

La Fiscalía también acusa a Bellorín de realizar el 13 de marzo de 2021 una publicación a través del perfil de Facebook Santos BOVG59 que en parte dice: **"Miserables vende patria, no les importa el sacrificio de nuestro pueblo. No al circo electoral de Ortega y sus zancudos CxL se venden a Ortega, CxL no representa al pueblo".**

Sin embargo, Fiscalía no demostró que las cuentas aludidas pertenecieran al campesino Bellorín ni cómo las publicaciones mencionadas pudieron haber causado "alarma, temor y zozobra entre" entre la población.

11.5.2 Exnovio de tiktoker Salma Flores condenado a 5 años de cárcel y a pagar 21 mil córdobas.

Kevin Alexander Reyes Leytón, exnovio de la tiktoker Salma Flores, había sido encontrado culpable de la filtración de imágenes íntimas de la joven.

Kevin Alexander Reyes Leyton, de 21 años, exnovio de la tiktoker nicaragüense **Salma Flores,** ha sido condenado a cinco años de prisión y a pagar una multa de 21,171 córdobas por el delito de filtración indebida de datos o información de carácter personal, según lo estipulado en la Ley de Ciberdelitos.

La sentencia fue dictada por la jueza del Segundo Distrito Penal de Juicio de Managua, Nadia Camila Tardencilla Rodríguez. A esta se le restará el año que ya lleva encerrado en la cárcel, pues ha permanecido detenido desde el 30 de junio del año pasado.

La familia de Reyes solicitó en varias instancias, incluida la Defensoría Pública, que se conociera la condena para poder continuar con el proceso de apelación.

En la documentación de la sentencia consta, según declaraciones de la víctima, que la joven y su exnovio acordaron tener relaciones sexuales en un motel de Managua

el 16 de octubre de 2021, mientras el condenado filmaba el acto. Sin embargo, este video y otras fotografías de carácter íntimo, que solo tenía el acusado en su celular**, fueron difundidos en las redes sociales, incluyendo Facebook, Twitter y WhatsApp, sin el consentimiento de Flores.**

Pornografía en grupos de mensajería:

Reyes, a través de su abogado defensor, había solicitado la pena mínima de tres años, mientras que el Ministerio Público pidió seis años. Finalmente, fue condenado a cinco años y deberá pagar la multa de 300 días, cuyo dinero será destinado al Sistema Penitenciario Nacional.

El caso de Salma Flores se ha convertido en uno de los más mediáticos debido a su popularidad en las redes sociales. Sin embargo, en el pasado se han reportado situaciones similares en las que los culpables no son castigados. E**n 2022, se hizo público la existencia de un grupo de Telegram titulado «**Nicaragua Caliente»**,** en el que hombres difundían contenido íntimo de mujeres sin su consentimiento, así como información privada como números de teléfono, direcciones y perfiles de redes sociales.

También víctima de ciberacoso:

Después de la filtración del video íntimo y las fotografías, la tiktoker denunció ser víctima de acoso cibernético por parte de perfiles falsos que la insultaban. Además, aseguró que sus padres fueron objeto de amenazas.

«Me decían que era prostituta, las cuentas que me mandaban las fotos son perfiles falsos… vulgarearon a mi hija, ya estaba mi hija en el suelo», dijo el padre de Flores ante la jueza del Segundo Distrito Penal de Managua, el año pasado.

Aunque el caso de Flores parece ser un punto de inflexión en los delitos de difusión de material privado sin el consentimiento de una de las partes involucradas.

EJEMPLO MÁS COMÚN DE DELITO INFORMÁTICO

De: Comunciado@Importante.2023 . <norvin2005@hotmail.com>
Enviado el: martes, 6 de junio de 2023 11:48
Para: Jacqueline Grisella Castillo Hernandez <JacquelineCastillo@banpro.com.ni>
Asunto: Notificaciones Banpro