Artículo original

Auge dela ciberdelincuencia en la sociedad moderna
The rise of cybercrime in modern society
Okakua kuaave ciberdelincuencia ko'ãga rupi.

*Natalia Belén López Brítez
https://orcid.org/0009-0000-8351-6181
Universidad del Norte. Ciudad del Este, Paraguay

Resumen

El artículo indica en primer término como la ciberdelincuencia ha ido escalando progresivamente en la sociedad. Así también, aborda las consecuencias que genera dicha forma de cometer hechos punibles, partiendo desde sus principales características y particularidades. De manera que, como método se utilizó el enfoque cualitativo, con diseño no experimental, de tipo documental, con un alcance descriptivo de corte transversal. Como objetivo se propuso determinar los tipos básicos de hechos punibles perpetrados a través de la informática; a fin de esbozar un análisis legislativo de las normas aplicables a dichos casos, a nivel nacional e internacional. También, se profundizó en lo que refiere a la jurisprudencia relativa a casos de ciberdelincuencia, tanto en la República del Paraguay como en el extranjero, verificando así qué tipo de situaciones se presentaron. Finalmente, se enfatizó en la gravedad de las acciones antijurídicas realizadas, a través de esta modalidad, pues allí radicó el punto central del trabajo investigativo. Se concluye que la ciberdelincuencia aumenta considerablemente con la evolución científica-informática, pues, se presentan nuevas formas de realizar los hechos punibles, lo cual resulta en un perjuicio notorio para la sociedad, por lo cual es fundamental ahondar esfuerzos en combatir este mal moderno.

Palabras claves: delito, legislación comparada, tecnología,jurisprudencia y ciberdelincuencia.

Recibido: 20/09/24 Aceptado: 21/11/24

*Egresada de la Universidad del Norte. Ciudad del Este. Paraguay. Email: natbelenlb@gmail.com

Abogada y Escribana Pública, egresada de la Universidad Privada del Norte, Diplomado en Derecho Laboral Fondo y Forma por la Escuela Judicial – Consejo de la Magistratura, Diplomado en Asistencia Jurídica en Materia Penal y no penal y Diplomado sobre Propiedad Intelectual por la Corte Suprema de Justicia. Relatora en el Tribunal de Apelación Penal Primera Sala de la VI Circunscripción Judicial de Alto Paraná.

ISSN 2415-5063 Versión impresa ISSN 2415-5071 Versión en línea
https://ojs.ministeriopublico.gov.py Contacto: dip.informaciones@ministeriopublico.gov.py

Abstract

The article first shows how cybercrime has been progressively escalating in society. It also addresses the consequences generated by this form of committing punishable acts, starting from its main characteristics and particularities. Thus, the qualitative approach was used as a method, with a non-experimental design, documentary type, with a cross-sectional descriptive scope. The objective was to determine the basic types of punishable acts perpetrated through informatics, in order to outline a legislative analysis of the rules applicable to such cases, at national and international level. Also, it was deepened in what refers to the jurisprudence related to cybercrime cases, both in the Republic of Paraguay and abroad, thus verifying what kind of situations were presented. Finally, emphasis was placed on the seriousness of the anti-legal actions carried out through this modality, since this was the central point of the research work. It is concluded that cybercrime increases considerably with the scientific-computer evolution, since new ways of committing punishable acts are presented, which results in a notorious damage to society, so it is essential to deepen efforts to combat this modern evil.

Key words: Cybercrime, compared legislation, jurisprudence, technology, modernity.

Ñemombyky

Ko kuatiañe'ẽme omombe'u mba'éichapa pe ciberdelincuencia okakua ohóvo mbegue katúpe ñande sociedad-pe. Upéicha avei oñe'ẽ mba'épa oheja hapykuerépe peichagua tembiapovai ojekastigáva, ohesa'ỹijo mba'épa péva, mba'émba'épa oguereko ko mba'e. Upéicha rupi ojeporu enfoque cualitativo ha imohendapy katu héra no experimental, ha ojejesarekopaite umi oñembokuatia va'ekuére ha upe guive omombe'u umi ojehúva tuichaháicha, umi kuatia oñemba'apo hague ojehechákuri ary 2000 guive 2010 peve. Umi ojejuhúva guive oñemohenda ha omoñe'ẽ mba´eichagua hecho punible-pa ojejapo ojeporukuévo informática; upe rire, ohesa'ỹijo leikuéra heseguáva ikatu kuaáva ojeporu umi káso rehe, tataha'e ko tetãpýre térã katu ambue tetãrupi avei. Upéicha avei oñembopypuku oñe'ẽvo jurisprudencia rehe ko Paraguái Retãme ambue tetãme guáicha, ohecha peteĩteĩ mba'eichagua itépa ojejapo hikóni. Ipahápe ojehechauka ijetu'uha ko mba'e heta mba'e ohógui leikuéra contra-pe, ojejapóva hikóni pe ciberdelincuencia rupive, ha upépe opyta ohesa'ỹijo ko investigación. Oñembyapu'ávo oje'ekuaa ko ciberdelincuencia heta hetaveha ojeguerojera háicha pe informática, ojejuhu juhuve mba'éichapa ojejapo hecho punible, péva ombyai mbaretéma ohóvo ñande sociedad-pe, upéicha rupi ningo tekotevẽte oñeñeha'ã jojapa ojehape joko haguã ko mba'e vai oguahẽva ko ára rupi.

Ñe'ẽ tee: Ciberdelincuencia, leikuéra, tecnología, sanción, modernidad.

Introducción

A través de los años se ha logrado numerosos avances científicos, con pasos agigantados, entre ellos, la informática, posicionándose en un creciente interés del ser humano que se ha ido acoplando progresivamente en la sociedad, en efecto, la digitalización es una realidad que se ajusta básicamente a todos los aspectos de la vida del hombre.

La tecnología permite que la sociedad avance, económica, social, académica y profesionalmente; por otro lado, también posibilita nuevas formas de cometer hechos punibles, allí es donde entra la ciberdelincuencia, que cada vez adquiere mayor profundidad con el paso del tiempo, dándose numerosas formas de quebrantar la ley y que representa un desafío al momento de investigar y procesar a los sujetos que realizan dichas actividades ilegales.

En ese marco es que corresponde, desde la normativa legal vigente en la República del Paraguay, estudiar como el auge de la ciberdelincuencia se instauró en la sociedad y cuáles son los principales delitos cibernéticos, pues actualmente la economía tiene una alta relación con los diversos sistemas informáticos digitales, así como los datos personales que al ser utilizados por terceros pueden generar gran perjuicio socio-económico, que posteriormente culmina en un daño a los derechos y garantías consagrados por las normas vigentes, por lo que debe ser objeto de estudio y resolución por parte del órgano jurisdiccional. En los últimos años, se presenta en la mayoría de los países a nivel mundial y el Estado paraguayo también afronta esta problemática en crecimiento.

En ese entendimiento, se plantea la siguiente interrogante ¿Cómo el progreso de la tecnología informática propicia el avance de la ciberdelincuencia?

De manera que, corresponde en primer término adentrarse en que consiste la ciberdelincuencia y como progresó con el paso del tiempo, para luego identificar los tipos de delitos cibernéticos, de qué manera se llevan a cabo, y describir las consecuencias que genera.

Por lo tanto, se realiza una verificación de la legislación pertinente aplicable al caso, también un análisis de la forma en la que se da en otros países, y como la observación en casos jurisprudenciales, tanto nacionales como extranjeros, los cuales permiten sentar las bases legales en distintos países, inclusive a nivel nacional, tendientes a evitar este tipo de hechos que cada vez son más constantes y producen un alto perjuicio social, económico y jurídico, pues amplía a una escala de mayor dificultad y alcance en cuanto a la forma de realizar hechos punibles.

Sobre la base de la consideración que antecede, se busca profundizaren el estudio del tema, tomando en cuenta la doctrina, jurisprudencia y legislación relativa a los delitos cibernéticos con la finalidad de alcanzar una perspectiva completa con datos determinados y específicos, que se dan gracias al detallado estudio, con base a los tres ejes principales mencionados previamente.

Con ese fin, se elaboró, en primer lugar, las ideas y conceptos necesarios para comprender adecuadamente el eje temático, para posteriormente adentrarse en el aspecto legal y finalmente, estudiar la aplicación de la legislación a casos concretos, mediante el análisis de jurisprudencias nacionales, complementando con el derecho comparado, tanto de las normas como de resoluciones que abordan el tema.

En tal sentido, el problema identificado es el crecimiento de la perpetración de hechos punibles a través de la informática, los denominados ciberdelitos, y consecuentemente el objetivo general es identificar la relevancia de las acciones antijurídicas, a través de la ciberdelincuencia.

La justificación del tema de estudio se denota tras el aumento respecto a este tipo de hecho punible, por medio de elementos informáticos, por lo cual resulta relevante, conocer los principales puntos y sus características. Así mismo, abarca la información jurídica y legislativa pertinente, que produzca un aporte relevante respecto al tema planteado, ofreciendo una óptica que se extiende a los factores sociales y económicos que hacen parte del conjunto en el que se dan las consecuencias de la ciberdelincuencia.

Metodología

El trabajo investigativo tiene enfoque cualitativo, con diseño no experimental, de tipo documental, con un alcance descriptivo y de corte transversal considerando los documentos revisados. Para obtener los datos, también se recurrió a la legislación vigente en la República del Paraguay, partiendo del Código Penal de 1997, con las respectivas modificaciones en la materia, así como de las normativas extranjeras relacionadas al objeto de estudio. Se realizó revisión de artículos de investigación con los aportes a la materia, a través de repositorios y revistas académicas.

Resultados

La ciberdelincuencia: generalidades

Es necesario delimitar la definición de ciberdelincuencia, pues se debe partir de las generalidades del concepto; en ese sentido, como bien precisa Arrazola Ruíz (2021) es el «fenómeno de la posibilidad de comisión de delitos o actos criminales, a través de sistemas informáticos» (p. 374), ya que es una figura bastante reciente en comparación a otras ramas, cuestiones o institutos de las ciencias jurídicas, por lo cual se debe determinar sus particularidades, pues bien, Punín Tandazo (2021) refiere: «mientras la sociedad en general daba sus primeros pasos en el ciberespacio, lo hacían también quienes esperan obtener un beneficio ilícito de los nuevos medios que se encontraban a su disposición». (p. 194)

A tal efecto, se precisa lo que hace parte a la ciberdelincuencia, por lo que es necesario hacer mención de las ideas de Peña Labrin (2023) en atención a que el ciberdelito se refiere a cualquier actividad delictiva que afecta a una computadora, una red informática o un dispositivo conectado a una red. Generalmente, estas acciones son cometidas por cibercriminales o *hackers*, motivados por intereses financieros. Sin embargo, la ciberdelincuencia también puede ser llevada a cabo por individuos u organizaciones, y algunos de estos cibercriminales forman parte de grupos criminales organizados. Estos grupos emplean sofisticadas técnicas de ingeniería social, y poseen habilidades tanto básicas como avanzadas en el ámbito informático.

El concepto de delito informático, en su definición más amplia, abarca situaciones en las cuales el componente informático es el objetivo de la actividad delictiva, como en el caso de accesos no autorizados a bases de datos, así como aquellas en las que la tecnología se utiliza como medio, para alcanzar fines ilícitos. Así, la ciberdelincuencia incluye tanto delitos tradicionales que se cometen con la ayuda de tecnologías informáticas, como aquellos delitos nuevos que solo son posibles gracias a los avances tecnológicos.

Por otro lado, los delitos informáticos en sentido estricto implican el ataque directo a bienes informáticos, tales como dañar *software* mediante la introducción de virus. En contraste, los delitos computacionales ocurren cuando la informática es utilizada como herramienta para cometer

otros tipos de delitos, como la suplantación de identidad o el *grooming,* entre otros. En casos menos frecuentes, el ciberdelito no tiene como principal objetivo obtener beneficios económicos, sino puede estar motivado por razones políticas o personales.

Considerando pues que la ciberdelincuencia es una novedosa manera de perpetrar hechos punibles, se resalta que en la actualidad presentan numerosas formas de efectuar un ciberdelito, al haber una gran cantidad de posibilidades, pueden realizarse desde básicamente cualquier dispositivo, que tenga acceso a la red, se pueden realizar estafas, alteración de datos, suplantación de identidad, acceso a cuentas bancarias, alteración de sistemas, entre otras formas más.

Sobre este punto en cuestión, es menester expresar con detalle las características fundamentales que hacen a la ciberdelincuencia, considerando la posición asumida por López Gorostidi (2022), por lo que es fundamental señalar que el hecho de que los delitos se cometan en el ciberespacio, les confiere características criminológicas únicas que los distingue de manera evidente de la delincuencia convencional. Estos rasgos, además, tienen implicaciones importantes en el ámbito dogmático, lo que debe ser considerado cuidadosamente al realizar un análisis, especialmente en lo que respecta a los objetivos de la pena que se busca imponer.

En primer lugar, como aspecto distintivo del uso de las tecnologías emergentes, destacamos el elevado porcentaje de la población mundial, que accede diariamente a internet, así como el creciente volumen de datos personales que los usuarios aportan al ciberespacio.

Una segunda característica técnica de las tecnologías de la información y la comunicación es la posibilidad de anonimato y la simulación de identidades que ofrece a los usuarios. Estos dos elementos son de los más significativos en internet y tienen un impacto notable en la toma de decisiones delictivas por parte de los cibercriminales. Por lo tanto, se presentan como factores clave en la expansión de las oportunidades delictivas dentro del ciberespacio.

En efecto, la ciberdelincuencia ha crecido bastante en los últimos años a nivel mundial, pues existen casos relacionados a hechos punibles que han llegado a instancias judiciales, conforme a la jurisprudencia nacional respecto del tema.

Principales tipos de delitos informáticos

Primeramente, es menester expresar que la informática permite diferentes posibilidades, pues, la digitalización de una innumerable cantidad de servicios ha permitido que la vida del ser humano sea más sencilla en muchos aspectos. Pero también, ha creado una dependencia a la tecnología, al adherirse de una forma simbiótica al hombre en sus distintas facetas, ya sea social, económica, personal, académica y profesional; a raíz de ello es que resulta muy factible, para quienes denotan una destreza en los conocimientos y habilidades, para el manejo de sistemas y dispositivos informáticos, permitiendo de esa forma la realización de los delitos cibernéticos.

En efecto, se entiende que con la aparición del ciberespacio, el hábitat delictivo ha crecido exponencialmente, pues la era de la información multiplica las oportunidades de los delincuentes. (Pons Gamón, 2017)

En tal sentido,corresponde que se enumeren algunos de los delitos más utilizados en los últimos tiempos y que generan graves perjuicios, se expresa en el cuadro:

Tabla 1
Definiciones de los conceptos relacionados a los delitos informáticos

Concepto	Definición
Los datos falsos o engañosos −*data diddling*−	Conocido también como introducción de datos falsos, es una manipulación de datos de entrada al computador, con el fin de producir o lograr movimientos falsos en transacciones de una empresa. Este tipo de fraude informático conocido también como manipulación de datos de entrada, representa el delito informático más común, ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición.
Manipulación de programas o los caballos de Troya −*Troyahorses*−	Es muy difícil descubrir y a menudo pasa inadvertida debido a que el delincuente tiene conocimientos técnicos en informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras, insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tienen conocimientos especializados en programación informática es el Caballo de Troya que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.
La técnica del salami −Salami *Technique/ Rounching Down*−	Aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina «técnica del salchichón» en la que «rodajas muy finas» apenas perceptibles de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra. Y consiste en introducir al programa unas instrucciones para que remita a una determinada cuenta los céntimos de dinero de muchas cuentas corrientes.
Falsificaciones informáticas	Como objeto: Cuando se alteran datos de los documentos almacenados en forma computarizada. Como instrumentos: Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de fotocopiadoras computarizadas en color, basándose en rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer reproducciones de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos, sin recurrir a un original, y los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de documentos auténticos.

Fuente: Acurio del Pino, 2016, p. 22.

Tabla 2 (continuación de la Tabla 1)
Definiciones de los conceptos relacionados a los delitos informáticos

Concepto	Definición
Manipulación de los datos de salida	Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude que se hace a los cajeros automáticos mediante la falsificación de instrucciones para la computadora, en la fase de adquisición de datos. Tradicionalmente, esos fraudes se hacían basándose en tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamente equipos y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de tarjetas de débito y tarjetas de crédito.
Pishing	Es una modalidad de fraude informático diseñada con la finalidad de robarle la identidad al sujeto pasivo. El delito consiste en obtener información tal como números de tarjetas de crédito, contraseñas, información de cuentas u otros datos personales por medio de engaños.

Fuente: Acurio del Pino, 2016, p. 22.

Estos delitos son complejos de realizar, en el sentido de que debe ser ejecutada por una persona con los conocimientos necesarios en las ciencias informáticas, a medida que realiza demuestra una mayor capacidad, y aumenta sus conocimientos y habilidades.

También, aumentará exponencialmente su peligrosidad en cuanto al nivel de efectos y consecuencias que genera, considerando que podrá realizar a una escala mayor, vulnerando sistemas de gran complejidad.

Normativa jurídica vigente en el Paraguay

Cabe resaltar en este punto, que la legislación penal, establece mediante la Ley n.° 1160/97, Código Penal, y sus modificaciones, hechos punibles que hacen a la ciberdelincuencia, partiendo de las disposiciones contenidas en el art. 146 c. Interceptación de datos, el cual regula la interceptación no autorizada de datos, imponiendo sanciones penales para quien, de forma ilegal y mediante el uso de medios técnicos, obtenga, transfiera o interfiera con datos que no le están destinados. La disposición busca proteger la confidencialidad de la información y prevenir el acceso indebido a datos personales o sensibles.

En el primer inciso, se establece que quien obtenga datos que no le han sido destinados, ya sea para su propio beneficio o para un tercero, estará cometiendo una infracción. Este tipo de conducta puede incluir prácticas como la obtención de información privada sin consentimiento, lo que pone en riesgo la seguridad y privacidad de los individuos.

El segundo inciso aborda la conducta de transferir datos de manera no pública, lo que podría implicar la divulgación o distribución indebida de información confidencial o sensible a personas no autorizadas. Este comportamiento también se considera una violación a la privacidad y seguridad de la información.

El tercer inciso se refiere a la transferencia ilegal de señales electromagnéticas de equipos de procesamiento de datos, una práctica que podría incluir la interceptación de comunicaciones o la manipulación de señales de dispositivos informáticos sin consentimiento.

En cuanto a las sanciones, el artículo establece una pena de hasta dos años de prisión o una multa, a menos que el hecho esté penado por otro artículo que contemple una pena mayor. Esto refuerza la gravedad de la infracción y la necesidad de una protección legal robusta frente a este tipo de delitos informáticos, en un contexto donde el acceso no autorizado a datos puede tener repercusiones graves tanto para las personas como para las organizaciones.

Así mismo, el art. 174 b. Acceso indebido a sistemas informáticos establece sanciones penales, para aquellos que accedan de manera ilegal a sistemas informáticos o sus componentes, ya sea utilizando una identidad propia o ajena, o excediendo los permisos otorgados. La pena puede incluir hasta tres años de prisión o una multa, dependiendo de la gravedad de la infracción. La finalidad de esta disposición es proteger la seguridad y privacidad de los sistemas informáticos, que hoy en día son una parte fundamental de las infraestructuras tecnológicas y de la gestión de información.

Además, el artículo aclara que un sistema informático no solo se refiere a un dispositivo individual, sino también a cualquier conjunto de dispositivos interconectados que trabajen juntos para procesar datos. Este concepto es crucial, ya que refleja la realidad de los sistemas informáticos modernos, que suelen estar compuestos por múltiples dispositivos interrelacionados, como servidores, redes y terminales. En resumen, el artículo busca abarcar una amplia gama de situaciones, desde el acceso a una computadora aislada hasta la intrusión en redes complejas, garantizando así una protección integral frente a la ciberdelincuencia.

El art. 174 tiene por finalidad la protección de la privacidad de las personas, en cuanto a su información se trata, todo lo que les pertenezca, ya sea de vida privada o laboral. Lo que se castiga consiste en el ingreso al sistema informático o a alguno de sus componentes, incluso cuando el autor lo realiza con su identidad propia.

El art. 175, en especial, lo que busca es resguardar a las instituciones públicas o sean estas, privadas, que utilizan sistemas de índole informáticos, para el cumplimiento de sus respectivos fines, ante los ataques de terceros contra equipos que sirven para el procesamiento de datos. El sabotaje, es considerado como «daño» (Casañas Levi, 2011).

Si bien no se trata de una normativa directa, éstas tienen estrecha relación con el tema de análisis del presente trabajo lo que consagra la Constitución Nacional (1992), en los siguientes términos, primeramente, el art. 33. «Del derecho a la intimidad. La intimidad personal y familiar, así como el respeto a la vida privada, son inviolables». Y en relación al art. 36 que refiere sobre el derecho a la inviolabilidad del patrimonio documental y de la comunicación privada. «El patrimonio documental de las personas es inviolable. Los registros, cualquiera sea su técnica…así como sus respectivas copias, no podrán ser examinados, reproducidos, interceptados o secuestrados sino por orden judicial para casos específicamente previstos en la ley…».

Legislación extranjera aplicable a la ciberdelincuencia

En este punto, es importante constatar la normativa aplicable a los casos de ciberdelincuencia en otros países con mayor avance tecnológico e informático, y por lo tanto, deben prever y regular con mayor énfasis todo lo relacionado al tema en cuestión, como bien se puede verificar de acuerdo a lo expresado en el siguiente cuadro:

Tabla 3

Legislación comparada en materia de ciberdelincuencia

País	Legislación
Alemania	Para hacer frente a la delincuencia relacionada con la informática y con efectos a partir del 1 de agosto de 1986, se adoptó la Segunda Ley contra la Criminalidad Económica del 15 de mayo de 1986 en la que se contemplan los siguientes delitos: Espionaje de datos (202 a), Estafa informática (263 a), Falsificación de datos probatorios (269) junto a modificaciones complementarias del resto de falsedades documentales como el engaño en el tráfico jurídico mediante la elaboración de datos, falsedad ideológica, uso de documentos falsos (270, 271, 273), Alteración de datos (303 a) es ilícito cancelar, inutilizar o alterar datos inclusive la tentativa es punible; Sabotaje informático (303 b). Destrucción de elaboración de datos de especial significado por medio de destrucción, deterioro, inutilización, eliminación o alteración de un sistema de datos. También es punible la tentativa. Utilización abusiva de cheques o tarjetas de crédito (266b). Por lo que se refiere a la estafa informática, la formulación de un nuevo tipo penal tuvo como dificultad principal el hallar un equivalente análogo al triple requisito de acción engañosa, producción del error y disposición patrimonial, en el engaño del computador, así como en garantizar las posibilidades de control de la nueva expresión legal, quedando en la redacción que, el perjuicio patrimonial que se comete consiste en influir en el resultado de una elaboración de datos por medio de una realización incorrecta del programa, a través de la utilización de datos incorrectos o incompletos, mediante la utilización no autorizada de datos, o a través de una intervención ilícita.
Francia	Ley n.° 88-19 del 5 de enero de 1988 sobre el fraude informático. Acceso fraudulento a un sistema de elaboración de datos (462-2), en este artículo se sanciona tanto el acceso al sistema como al que se mantenga en él y aumenta la sanción correspondiente si de ese acceso resulta la supresión o modificación de los datos contenidos en el sistema o resulta la alteración del funcionamiento del sistema. Sabotaje informático (462-3), se sanciona a quien impida o falsee el funcionamiento de un sistema de tratamiento automático de datos. Destrucción de datos (462-4), en este artículo se sanciona a quien intencionadamente y con menosprecio de los derechos de los demás introduzca datos en un sistema de tratamiento automático de datos o suprima o modifique los datos que este contiene o los modos de tratamiento o de transmisión. Falsificación de documentos informatizados (462-5), en este artículo se sanciona a quien de cualquier modo falsifique documentos informatizados con intención de causar un perjuicio a otro. Uso de documentos informatizados falsos (462-6), en este artículo se sanciona a quien conscientemente haga uso de documentos falsos haciendo referencia al artículo 462-5.

Tabla 4 (Continuación, Tabla 3)
Legislación comparada en materia de ciberdelincuencia

País	Legislación
Argentina	Ley n.° 25326 de protección de datos personales. Ley n.° 26.904 de *grooming*. La Ley Nacional n.° 26388 de Delitos Informáticos incorpora y tipifica los delitos informáticos al Código Penal Argentino con el objeto de regular las nuevas tecnologías como medios de comisión de delitos. Los delitos informáticos incorporados son: Violación, apoderamiento y desvío de comunicación electrónica (art. n.° 153, párrafo 1º C. P.); Intercepción o captación de comunicaciones electrónicas o telecomunicaciones (art. n.° 153, párrafo 2º C. P.); Acceso a un sistema o dato informático (art. n.° 153 bis C. P.); Publicación de una comunicación electrónica (art. n.° 155 C. P.); Acceso a un banco de datos personales (art. n. ° 157 bis, párr. 1º C. P.); Revelación de información registrada en un banco de datos personales (art. n.° 157 bis, párrafo 2º C. P.); Inserción de datos falsos en un archivo de datos personales (art. n.° 157 bis, párrafo 2º C. P.); anteriormente regulado en el art. n.° 117 bis, párr. 1º, incorporado por la Ley de Hábeas Data; Fraude informático (art. n.° 173, inciso 16 C. P.); Daño o sabotaje informático (arts. n.° 183 y 184, incisos 5º y 6º C.P.).
Chile	En junio de 1993 entró en vigencia la Ley n.° 19.223, sobre delitos informático. Tiene como finalidad proteger a un nuevo bien jurídico como es: "la calidad, pureza e idoneidad de la información en cuanto a tal, contenida en un sistema automatizado de su tratamiento y de los productos que de su operación se obtengan". Es una ley especial, extra-código y consta de 4 artículos, que se enuncian a continuación. Art. 1. "El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo. Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo". Art. 2. "El que, con ánimo de apoderarse, usar o conocer indebidamente la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio". Art. 3. "El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio". Art. 4. "El que maliciosamente revele o difunda los datos contenidos en un sistema de información sufrirá la pena de presidio menor en su grado medio. Si quien incurriere en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado". Se contempla los delitos informáticos de sabotaje y espionaje informáticos, aunque no de una forma clara. Así pues, en el artículo 1, el inciso primero alude a los daños que se puedan cometer contra el *hardware*, inutilizándolo, por lo que no se trataría de un delito informático, sino más bien de un delito de daños convencional. Es en el art. 3° donde se encontraría la figura del sabotaje informático al sancionar al que maliciosamente altere, dañe o destruya los datos contenidos en un sistema.

Fuente: Acurio del Pino, 2016, pp. 34-39.

Análisis jurisprudencial nacional e internacional

Corresponde en tal sentido señalar las resoluciones nacionales e internacionales, partiendo de las emanadas del Poder Judicial. Primeramente, se trae a colación el caso de «Diego Ramón Espínola Medina y otros s/ Acceso Indebido a Sistemas Informáticos».

Tabla 5

Sentencia definitiva n.° 39 dictada en el marco de una causa relacionada a la ciberdelincuencia de Asunción en el 2021

Caso n.° 1 Diego Ramón Espínola Medina y otros s/ Acceso Indebido a Sistemas Informáticos	
Hechos	Para obtener este beneficio indebido se ingresó con el perfil del Sr. Antonio Brítez a la banca web de los bancos con su clave de acceso y se manipuló su token. Así también cabe destacar que, en septiembre del año 2019, se cargó un asiento en el software corporativo contable de sistema de gestión GFIS, *Global Financial Information System* que causó fluctuaciones anormales en los saldos de cuentas de balance. Este asiento fue identificado con el Jornal ID: ESPIND010 y Jornal Date: 2019-09- 27 y correspondería a una operación fraudulenta para justificar la falta de fondos distribuibles de la empresa, realizada por Diego Espínola.
Pruebas principales	1. Extractos bancarios correspondientes a los encausados Diego y Marta. 2. Impresión de los correos electrónicos respecto a las transferencias realizadas. 3. Copia autenticada realizada ante escribanía pública sobre los equipos utilizados por los encausados, memorándum de los análisis preliminares de las operaciones realizadas. A más de la admisión de los acusados sobre los hechos.
Calificación de la conducta	Arts. 248 Alteración de datos relevantes de prueba, 174 b Acceso indebido a sistemas informáticos, y 188 Estafa mediante sistemas informáticos del CP modificado por Ley n.° 4439/11 en concordancia con el art. 29 inc. 1 en calidad de autor, del citado cuerpo normativo.
Condena	Dos años con suspensión a la ejecución de la condena, por considerar que se trataban de personas que no poseen antecedentes, a más de que admitieron los hechos.

Fuente: Sentencia Definitiva n.° 39 (2021, 07 de junio). Juzgado Penal de Garantías n.° de Asunción.

Tabla 6
Sentencia Definitiva n.° 324 dictada en el marco de una causa relacionada a ciberdelincuencia de Asunción en el 2018

Caso n.° 2 Dante Daniel Pérez sobre Alteración de Datos y Otros	
Hechos	El ciudadano Dante Daniel Pérez, teniendo en cuenta que el Sr. Ignacio Elizalde en representación de la Empresa *Looking Satelital* ha celebrado un contrato de prestación de servicio con el Sr. Dante Daniel Pérez, quien le vendería un *software* para la prestación de servicios de rastreo, a ser controlado por el acusado desde su domicilio sito en las calles Agustín Barrios n.° 1174, Barrio Carmelitas de la ciudad de Asunción. Habiendo transcurrido un tiempo y tenido la empresa *Looking Satelital* diversos tipos de quejas por el mal servicio que brindaba, debido a que el software nunca era terminado por el acusado, el Sr. Ignacio Elizalde en compañía con la Sra. Lea Cena, gerente de la empresa, citan al acusado en la empresa sito en Alas Paraguayas n.° 633 para el 15 de noviembre de 2013, donde le comunican el término de la relación laboral, por no haber completado el *software*, luego entre el 20 y el 26 de noviembre de 2013, la empresa recibe numerosas llamadas de los clientes manifestando que no podían ver sus vehículos, ante esta situación, la Sra. Lea Cena ingreso al sistema donde efectivamente corroboró que se habían borrado datos de la base de datos, luego de las averiguaciones se pudo determinar que la IP 186.2.225.193 se encontraba a nombre de Giulia Livieres Savino con C. I. n.° 3351857 quien es esposa del hoy acusado, fijando como domicilio la calle Agustín Barrios n.° 7174, que es el domicilio perteneciente al acusado Dante Daniel Pérez, por lo que al tener el señor Dante Pérez los usuarios y contraseñas del servidor de la empresa *Looking*, además de hacer trabajos remotos desde su domicilio, se pudo determinar que el acusado fue el autor de esos ataques que sufrió la empresa en cuestión.
Pruebas principales	1. Escrito presentado por el Sr. Ignacio Martín Elizalde González, acompañado con el informe elaborado por el informático Max Sirio Soarez, en fecha 24 de enero de 2014, a través del cual informó que en fecha 19 de enero, por medio del IP 186.2.255.193 (utilizada por el acusado) se ingresó de manera remota al sistema de rastreo satelital de la empresa y se procedió al borrado de contraseña de los usuarios. 2. Informe de la empresa TIGO en donde puede verse el IP utilizado para el ataque y daba conexión con el domicilio del acusado. 3. Informe técnico informático de coordinación de apoyo técnico de la unidad especializada de delitos informáticos sobre los datos contenidos en el disco duro externo utilizado por el acusado que tiene los archivos, datos y carpetas de los servidores de la empresa denunciante. 4. La pericia realizada a la notebook de la marca Toshiba de color negro con número de serie YC273110Q. 5. Pericia realizada al disco duro externo, del cual pudieron extraerse que los correos asociados corresponden al señor Dante (en base a esta pericia que efectivamente las cuentas y la IP asociadas al señor Dante Daniel Pérez, han ingresado al dominio del servidor, dando instrucciones de ejecución de comandos).

Tabla 7 (Continuación de la Tala 6)
Sentencia Definitiva n.° 324 dictada en el marco de una causa relacionada a ciberdelincuencia en Asunción en el 2018

Caso n.° 2 Dante Daniel Pérez sobre Alteración de Datos y Otros	
Calificación de la conducta	Arts. 174 Alteración de datos, 174b Acceso indebido a sistemas informáticos y 175 Sabotaje de computadoras del CP y su Ley n.° 4439/11en concordancia con el art. 29 inc. 1° del mismo cuerpo legal.
Condena	2 años y 6 meses.

Fuente: Sentencia definitiva n.° 324 (2018, 19 de setiembre) Tribunal de Sentencia Colegiado de Asunción, n.° 1

En cuanto al estudio internacional, en Argentina, se encuentra un fallo que se refiere al tema objeto de análisis del presente trabajo, destacando la partes: V. C. E. s/ infracción arts. 153 bis primer párr. y 149 ter inc. 1 del Código Penal, resuelto por el Tribunal Oral en lo Criminal Federal de Santa Fe, de fecha 6 de septiembre de 2022, en donde se condena a quien se introdujo en el sistema informático de un medio periodístico e insertó virus en alguna de sus terminales o procesadores y publicó en su página a la vista del publicó un mensaje específico.

Gravedad de las acciones antijurídicas realizadas a través de la ciberdelincuencia

En atención a todo lo antes dicho, se comprende que, la informática en manos equivocadas es un arma nefasta, pudiendo causar todo tipo de daños, sea económico, social, personal, académico o profesional, desde una gran distancia y en muchas ocasiones desde el anonimato, perjudicando gravemente a las víctimas.

Por ello es que, ha generado sin dudas un gran cambio en la sociedad, y también en el derecho, pues evoluciona a la par del hombre para regular su vida en relación a los demás, es preciso lo dicho por Pérez Arias (2021) cuando indica «la informática es sin lugar a dudas, uno de estos giros copernicanos que ha revolucionado no solo el Derecho Penal tradicional −incluyendo nuevos métodos o medios comisivos−, sino la misma civilización en su conjunto» (p. 177).

Si bien es cierto que esta modalidad de hecho punible es reciente en comparación a otras más antiguas como el robo o el homicidio, no se puede negar que las consecuencias genera un menoscabo al bien jurídico tutelado por la normas, ya que normativamente se las ubica en el Capítulo I del CP «Hechos punibles contra la propiedad de los objetos y otros derechos patrimoniales», y

que debe ser ampliamente regulado y controlado por parte del Estado, pues la red es un universo digital que permite cualquier tipo de conducta, acción o contenido nocivo.

Por ello, muchos países han realizado esfuerzos jurídicos y legislativos para combatir este tipo de acciones que afectan a los ciudadanos y son contrarias al orden jurídico.

En tal sentido, en el continente europeo como explica Quevedo González (2017) se encuentran:

> **Centro Europeo de Ciberdelincuencia de Europol**
>
> La Estrategia de seguridad interior de la Unión Europea en acción, adoptada el 22 de noviembre de 2010, por la Comisión estableció la creación del Centro Europeo de **Ciberdelincuencia de Europol** (EC3) como una de las medidas destinadas a proteger a los ciudadanos de los ciberdelitos. Complementó a las propuestas legislativas, como la Directiva relativa a los ataques contra los sistemas de información y la Directiva relativa a la lucha contra la explotación sexual de la infancia en internet y la pornografía infantil. La misión en la lucha contra la ciberdelincuencia es desarticular las operaciones de las redes delictivas organizadas que cometen ciberdelitos. Apoya y coordina muchas de las operaciones e investigaciones llevadas a cabo por las autoridades de los Estados miembros.
>
> **Eurojust**: es la Unidad de Cooperación Judicial de la Unión Europea, creada en el año 2002, con el objetivo de estimular y mejorar la coordinación de las investigaciones y el ejercicio de las acciones penales, así como la cooperación entre las autoridades competentes de los Estados miembros en relación a la delincuencia transfronteriza, entre la que se incluye la ciberdelincuencia como una de sus prioridades.
>
> **ENISA:** es la Agencia Europea para la red y la seguridad de la información un centro de expertos para la ciberseguridad en Europa (pp. 132-133).

Se observa que en Europa se crearon tres instituciones encargadas a nivel continental, al margen de las diversas otras que son de índole nacional, ya se puede denotar voluntad de política de hacer frente al fenómeno de la ciberdelincuencia en la sociedad moderna.

En esa línea, las acciones deben tener concordancia con la gravedad de esta modalidad delictiva a través de las tecnologías,al respecto Quevedo González (2017) expresa:

> … el internet ha influido significativamente en la actividad criminal al generar nuevas formas de criminalidad y servir como instrumento para la comisión de otros delitos tradicionales. Por ello, la investigación del denominado ciberdelito exige conocer las características técnicas básicas de internet (p. 401).

En efecto, esta circunstancia no se limita a Europa o América, sino en la mayoría de los continentes, pues la ciberdelincuencia se ha expandido a nivel estratosféricos, como bien señalan Flores Villacrés et al. (2014) con los datos siguientes:

> La delincuencia informática mundial tiene un costo de 114 mil millones de dólares anuales, se determinó que más de dos tercios de los adultos en línea (69 %) han sido víctimas de la ciberdelincuencia alguna vez en la vida. Cada segundo, 14 adultos son víctimas de un crimen cibernético, lo que deja como resultado más de un millón de víctimas del cibercrimen todos los días (p. 4).

En tal sentido, la mayoría de los hechos punibles tipificados en la norma son de suma relevancia pues tienen una notoria incidencia en el orden público, se debe destacar que la ciberdelincuencia es una modalidad criminal ventajosa para los sujetos que realizan dichos actos, pues dar con los autores requiere de un gran esfuerzo y utilización de muchos recursos humanos, financieros y tecnológicos para lograr llevarlos ante la justicia.

Conclusión

Al ser un tema muy amplio, pero a la vez delimitado, alcanzar una conclusión sobre el mismo requiere de un trabajo de análisis y síntesis, debido a las aristas que se presenta a nivel jurídico, social y económico −principalmente−. En consecuencia, se puede afirmar que se logró abarcar los principales puntos determinantes que hacen al trabajo, y que permite esbozar un cierre.

En tal sentido, la ciberdelincuencia se va posicionando cada vez más en la sociedad paraguaya, como a nivel mundial, destacando la gran magnitud de esta forma de criminalidad.

Las diversas tipologías de cometer un hecho punible mediante la utilización de la informática van en aumento, pues tiene sus propias características y también se puede utilizar para ejecutar otros tipos de hechos punibles ya tipificados, dándose así una doble faceta en cuanto a la realización de la ciberdelincuencia, y su más que complicada manera de contrarrestarla. A falta de tipificación, la conducta no constituye un hecho punible, por lo que se necesita revisar la redacción para una mejor comprensión de la idea de la autora.

Constituye un desafío jurídico y social combatir este tipo de criminalidad, pues requiere de preparación en el estudio de la informática para resolver los casos, así como también para evitarlos, por lo que no se limita únicamente a los saberes de las ciencias jurídicas, debiendo así darse cada vez más especializaciones en el área, a fin de cubrir este tipo de situaciones.

Se concluye que esta modalidad delictiva aumentó con el avance tecnológico e informático, y esto podría ir evolucionando aún más, por lo que corresponde necesariamente tomar las medidas preventivas y punitivas para lograr salvaguardar los derechos de las personas, a fin de evitar que se vean perjudicas por los hechos punibles efectuados a través de la informática.

Recomendación

Al realizar una recomendación, lo evidente es que se deben fortalecer los mecanismos de seguridad de la mayoría de los sistemas públicos y privados, a fin de evitar que pueda accederse a dichas plataformas y, también que cada individuo tome las precauciones debidas con sus datos personales que se encuentran en riesgo de ser vulnerados.

En tal sentido, se debe fomentar la creación de instituciones encargadas de salvaguardar, informáticamente, los datos y sistemas, dotándolos de recursos pertinentes, como se ha visto en el continente europeo y al margen del esfuerzo estatal, se debe concientizar a la ciudadanía en lo que respecta a la prevención, de manera a tener un cuidado personal que ayude a combatir este tipo de acción antijurídica.

Teniendo en cuenta, que se debe profundizar en lo que respecta a la legislación nacional vigente, ampliando el alcance y posibilidades mediante la norma formar, crear y potenciar los mecanismos posibles, a fin de detener, sancionar y erradicar el tipo de hecho punible.

Referencias

Acurio Del Pino, S. (2016). Delitos Informáticos: Generalidades. Universidad Central del Ecuador. Recuperado de http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Arrazola Ruiz, S. (2021). La ciberdelincuencia como fenómeno jurídico. Su tratamiento procesal. Revista Aequitas -Estudios sobre historia, derecho e instituciones, Núm. 18. pp. 371-402.

Casañas Levi, J. F. (2011). Código Penal de la República del Paraguay Comentado – Libro Segundo Parte Especial. Asunción: Editorial La Ley Paraguaya.

Casañas Levi, J. F. (2011). Código Penal de la República del Paraguay Comentado – Libro Segundo Parte Especial (Continuación) – Libro Tercero Parte Final. Asunción: Editorial La Ley Paraguaya.

Congreso de la República del Paraguay. (1997). Ley n.° 1160 - Código Penal. Asunción: Gaceta Oficial de la República del Paraguay.

Congreso de la República del Paraguay. (2011). Ley n.° 4439 que modifica y amplia varios artículos de la Ley n. ° 1.160/97 "Código Penal". Asunción: Gaceta Oficial de la República del Paraguay.

Convención Nacional Constituyente. (1992). Constitución Nacional del Paraguay. Asunción: Gaceta Oficial de la República del Paraguay.

Flores Villacrés, E., Asanza Molina, M. &BerronesMiguez, M. (2014). Ciberdelincuencia un mal que afecta a la sociedad actual.Contribuciones a las Ciencias Sociales - Septiembre. www.eumed.net/rev/cccss/29/ciberdelincuencia.html

López Gorostidi, J. (2022). Sobre el alcance de los fines de la pena en el fenómeno criminal de la ciberdelincuencia. Revista Chilena de Derecho y Tecnología Vol. 11 Núm. 1, pp. 121-146. DOI 10.5354/0719-2584.2022.60913

Juzgado Penal de Garantías de Asunción, n.°1. (2021, 07 de junio). Sentencia Definitiva n.° 39 (D. R. E. M. y otros s/ acceso indebido a sistemas informáticos y otros). Corte Suprema de Justicia de la República del Paraguay.

Peña Labrin, D. E. (2023) Ciberdelitos y criminalidad informática. Rol de la prevención en la expansión de la ciberdelincuencia. Revista Iberoamericana de Derecho Informático (Segunda Época) n.° 13, pp. 57-72.

Pérez Arias, J. (2021). Cibercriminalidad: hacia la nueva realidad -virtual- del Derecho Penal. Revista Internacional de Doctrina y Jurisprudencia, Volumen 26. pp. 175-193.

Pons Gamón, V. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. URVIO, Revista Latinoamericana de Estudios de Seguridad, Núm. 20. pp. 80-93.

Punín, P. (2021). Breve aproximación a la ciberdelincuencia desde una perspectiva criminológica. Revista Ruptura de la Asociación Escuela de Derecho PUCE. Edición 2021. pp. 191-230.

Quevedo González, J. (2017). Investigación y prueba del ciberdelito. Universitat de Barcelona. Recuperado de http://hdl.handle.net/2445/128112

Tribunal de Sentencia Colegiado de Asunción, n.° 1. (2018, 19 de septiembre). Sentencia Definitiva n.° 324 (D. D. P. s/ alteración de datos y otros). Corte Suprema de Justicia de la República del Paraguay.