REGULACIÓN DE LA CIBERSEGURIDAD[1]

Aldo Fabrizio Modica Bareiro[2]

Resumen

El presente artículo tiene como objetivo realizar un estudio de la literatura legal sobre la ciberseguridad, tanto a nivel internacional como local. El estudio abarca desde el concepto y alcance del término ciberseguridad, pasando por su vinculación con el Tratado de Budapest sobre ciberdelincuencia y las principales prácticas de delitos de ingeniería social. También se analiza la regulación sobre ciberseguridad a nivel Unión Europea, Estados Unidos, América, y finalmente Paraguay, de manera a identificar cuáles son las principales normativas vigentes vinculadas al tema en cuestión.

Abstract

The objective of this article is to carry out a study of the legal literature on cybersecurity, both at an international and domestic level. The study covers the concept and scope of the term cybersecurity, through its connection with the Budapest Treaty on cybercrime and the main practices of social engineering crimes. The regulation on cybersecurity is also analyzed at the European Union, United States, America, and finally Paraguay, identifying the main regulations that are in force related to the subject in question.

Palabras claves: Ciberseguridad; Leyes; Unión Europea, Estados Unidos; América; Paraguay

Keywords: Cybersecurity; Laws; European Union, United States; America; Paraguay

[1] Este trabajo fue realizado en el marco del proyecto PINV15-165 "Yo Digital: Educación y Desarrollo de Infraestructuras en Ciberseguridad y Privacidad", financiado por el CONACYT a través del Programa PROCIENCIA con recursos del Fondo para la Excelencia de la Educación e Investigación – FEEI del FONACIDE

[2] Abogado por la Universidad Católica Nuestra Señora de la Asunción. Doctor en Derecho por la Universidad Austral de Buenos Aires. Magister en Docencia en Educación Superior por la Universidad Católica Nuestra Señora de la Asunción. Magister en Propiedad Intelectual por la Universidad Austral de Buenos Aires (Medalla de oro). Coordinador de investigación de la FCJD.

1. Introducción

La ciberseguridad constituye hoy en día en uno de los mayores desafíos a nivel mundial, en el que tanto las personas como las organizaciones -especialmente los Estados- están involucrados activamente en su protección. Una de las formas más efectivas de hacer frente a esta problemática es regulando un mínimo de pautas comunes que permitan establecer una base legal para su efectivo cumplimiento.

Es por ello, por lo que se analizará primeramente lo que se entiende por ciberseguridad -tanto en su sentido técnico como legal- con la finalidad de adoptar una definición que permita precisar su contenido, alcance y disposiciones, teniendo en cuenta de que no existe un consenso generalizado sobre el tema. Se recurrirán a las principales definiciones de los organismos internacionales, los Estados, y otras instituciones, especialmente porque no existe una definición legal sobre el término a nivel internacional ni local.

En cuanto a ciberseguridad en sentido general, se establecerá su regulación a nivel internacional, siendo necesario para ello recurrir a lo establecido en el Tratado de Budapest sobre Ciberdelincuencia. Asimismo, se verán cuáles son las principales prácticas de ciberdelincuencia o delitos de ingeniería social que en los últimos tiempos a nivel mundial han afectado las estructuras en los sistemas de información y comunicación. El presente estudio no tratará las cuestiones que hacen a la ciberseguridad y su vinculación con la ciberdefensa, el ciberespionaje, el ciberterrorismo, entre otros.

A continuación y adentrándonos en un análisis regional, se verá cómo está regulada la ciberseguridad en la Unión Europea por medio de dos directivas aprobadas sobre el tema, y otras propuestas de mejoras. La primera directiva se refiere a los ataques contra los sistemas de información, y la segunda está destinada a garantizar un elevado nivel común de seguridad de las redes y sistemas de información. Luego, en lo que respecta a Estados Unidos, se verán regulaciones específicas como la ley Federal de Gestión de la Seguridad de la Información, la Ley de Intercambio de Información de Ciberseguridad, y otras normativas referidas a industrias o sectores específicos.

Para el análisis de la regulación en América, veremos los principales documentos con que se cuenta tanto a nivel de la OEA como del MERCOSUR. Finalmente, en lo que respecta al análisis de la ciberseguridad en Paraguay, haremos un repaso de las principales normativas que tratan diversos aspectos vinculados al tema, haciendo

especial énfasis en el Plan Nacional de Ciberseguridad de la SENATIC, en el Código Penal Paraguayo, la ley de Comercio Electrónico, entre otras normativas vigentes.

2. Ciberseguridad

2.1 ¿Qué es la ciberseguridad?

En primer lugar, antes de adentrarnos al análisis jurídico de la ciberseguridad y sus diversas normativas aplicables, conviene que definamos el término en cuestión, ya que no existe un consenso generalizado que permita adoptar una definición precisa sobre su contenido, disposiciones y alcances, término que por cierto no está regulado jurídicamente a nivel internacional -mucho menos a nivel local- y que incluso genera confusión entre los mismos expertos.

Para la Unión Internacional de Comunicaciones (UIT), la ciberseguridad "es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno[3]". Esta definición amplia de ciberseguridad parecería estar limitada a una función preventiva, es decir, como políticas y acciones llevadas a cabo para proteger las redes interconectadas del acceso y modificación -ilegítimo o no-autorizado por terceros. Sin embargo, vemos que la ciberseguridad también debe garantizar la estabilidad, el buen funcionamiento de los sistemas y el resguardo de la información una vez sufridas las amenazas o incidentes, es decir, a *posteriori*.

Para el Departamento de Seguridad de los Estados Unidos, la definición standard de ciberseguridad tiene que ver con "la actividad o proceso, habilidad o capacidad, o estado por el cual los sistemas de información y comunicación y la información contenida en ellos están protegidos y/o defendidos contra daños, uso o modificación no autorizada o explotación"[4]. Otra definición más, acotada en el mismo sentido, establece que la ciberseguridad es "la protección de activos de información a través del tratamiento de amenazas que ponen en riesgo la información que es procesada,

---

[3] Recomendación UIT-TX.1205 (04/2008) - *Aspectos generales de la ciberseguridad*, 9. En https://www.itu.int/rec/T-REC-X.1205-200804-I/es

[4] *Definition of Cybersecurity: The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation. National Initiative for Cybersecurity Careers and Studies (NICCS).* En https://niccs.us-cert.gov/glossary#C.

almacenada y transportada por los sistemas de información que se encuentran interconectados[5]".

Estas últimas dos definiciones están más acorde con la tendencia actual de limitar el concepto exclusivamente al resguardo de los sistemas y los datos informáticos, prescindiendo del medio por el cual éstos se llevan a cabo y por sobre todo defendiendo la neutralidad tecnológica de la red, que según la Comisión Interamericana de Derechos Humanos (CIDH) de la Organización de los Estados Americanos (OEA), "para evitar un concepto amplio que pueda conducir a la criminalización del uso de Internet, el concepto de ciberseguridad se contrae a la protección de una serie de bienes jurídicos, como la infraestructura y la información almacenada o de cualquier manera administrada a través de Internet, pero no al medio tecnológico empleado para cometer un ilícito de cualquier naturaleza[6]".

De todas las definiciones mencionadas, podemos extraer que la ciberseguridad se refiere esencialmente a la protección y salvaguarda de las infraestructuras y los datos almacenados en ellas, que poseen un valor para las organizaciones y los usuarios, y se encuentran expuestas a riesgos o amenazas debido a su tratamiento digital, especialmente a través de internet. En ese sentido, tanto los usuarios como las organizaciones –incluido el propio Estado- deben establecer mecanismos que comprendan aplicaciones, servicios y demás gestiones de los activos, con el fin de resguardar la información en el manejo del ciberespacio. La pérdida de información y los incidentes causados por amenazas en la red o los ciberataques, traen consigo una serie de consecuencias que afectan directamente la confianza de las personas, la economía e incluso la propia seguridad de los Estados.

Para hacer frente a estas amenazas y mitigar los posibles daños que significarían los ciberataques en un contexto tanto local como internacional -como lo es internet- los gobiernos desarrollan estrategias, políticas y legislaciones especiales para combatir desde un entorno digital a este flagelo cada vez más mayor, peligroso, y con efectos muy devastadores en la sociedad.

Finalmente, algunas voces sostienen que debe ampliarse el concepto de ciberseguridad al de seguridad digital. Este último abarcaría a la conectividad, los sistemas de

[5] Definición dada por parte de ISACA (*Information Systems Audit and Control Association* – Asociación de Auditoría y Control sobre los Sistemas de Información). En https://www.icemd.com/digital-knowledge/articulos/definicion-ciberseguridad-riesgo/

[6] Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos de la OEA, Libertad de Expresión e *Internet*, 2013, 59. En http://www.oas.org/es/cidh/expresion/docs/informes/2014_04_08_internet_web.pdf

información y la integración de plataformas de soportes y operativas. En otras palabras, "ampliar el ámbito de ciberseguridad a todo el entorno corporativo (incluyendo procesos y personas), y extenderlo más allá de la organización (incluir a *partners* y clientes)[7]". En igual sentido se pronuncia la OCDE[8].

2.2 Regulación jurídica de la Ciberseguridad a nivel internacional

El primer tratado internacional que regula aspectos vinculados a la ciberseguridad es el Convenio sobre Ciberdelincuencia[9] -conocido también como Convenio de Budapest- cuyo objetivo es aplicar una política penal común encaminada a la protección de la sociedad contra el cibercrimen[10], especialmente mediante la adopción de una legislación adecuada y el fomento de la cooperación internacional. El mismo fue aprobado primeramente por el Comité de Ministros del Consejo de Europa en el 2001 y entró en vigor en el 2004, posteriormente para el año 2006 fue incorporado el Protocolo Adicional al Convenio sobre Ciberdelincuencia Relativo a la Penalización de Actos de índole Racista y Xenófobos, y actualmente se encuentra ratificado por 56 países[11], entre los que podemos citar a los países de la Unión Europea, Estados Unidos, Canadá, Japón, Sudáfrica, la mayoría de los países latinoamericanos - incluido Paraguay[12]-, entre otros.

El Convenio establece que los Estados deberán adoptar en sus respectivas legislaciones penales tanto medidas sustantivas o de fondo como procesales o de forma para combatir

---

[7] https://www.icraitas.com/blog/2017/3/17/ciberseguridadyseguridaddigital.

[8] "La Organización para la Cooperación y el Desarrollo Económicos (OCDE) ha modificado el término de Ciberseguridad a Seguridad Digital en el Plan Nacional de Seguridad digital de Colombia, que en su primera parte fue desarrollado con el apoyo de la Organización de Estados Americanos (OEA). "Sería interesante analizar esta experiencia, ya que el Gobierno actual de Paraguay está trabajando firmemente en formar parte de esta organización" (Tecnología & Comunidad TEDIC, *Problemas serios y desafíos que tiene el Plan de Ciberseguridad en Paraguay*, Junio de 2016, Asunción, 4, en https://www.tedic.org/wp-content/uploads/sites/4/2016/06/observaciones-sobre-el-plan-de-ciberseguridad_v14jun-.pdf. El 02/03/2017 Paraguay se convirtió en el miembro número 52 del Centro de Desarrollo de la OCDE, en http://www.oecd.org/dev/paraguay-convierte-miembro-centro-desarrollo-ocde.htm.

[9] La ciberdelincuencia puede ser entendida de dos maneras. Así tenemos que la "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. En sentido general, ciberdelincuencia (delitos relacionados con las computadoras) comprende cualquier comportamiento ilícito cometido por un medio de un sistema informático o una red de computadoras, o relacionado con éstos, incluidos delitos tales como posesión ilícita y la puesta a disposición o distribución de información mediante sistemas informáticos o redes de computadoras". Marco GERKCE, *Comprensión del ciberdelito: fenómenos, dificultades y respuestas jurídica*, informe del Departamento de Infraestructura, Entorno propicio y Ciberaplicaciones de la Oficina de Desarrollo de las Telecomunicaciones de la UIT, 2014, 9, en https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime2014_S.pdf.

[10] También conocido como "ciberelito". Se refiere a toda acción típica, antijurídica y culpable, que se da por vías informáticas o tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de internet.

[11] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=hPsy1oRF

[12] Ratificado el 20 de diciembre del 2017, a través de la Ley 5994/17.

la ciberdelincuencia. En relación a las normativas penales de fondo, los Estados deberán establecer los siguientes delitos: a) delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos[13]: acceso ilícito, la intercepción ilícita, ataques a la integridad de los datos, ataques a la integridad del sistema, abuso de los dispositivos; b) delitos informáticos: falsificación informática y fraude informático; c) delitos relacionados con el contenido: pornografía infantil; d) delitos relacionados con infracciones de propiedad intelectual y de los derechos afines: derechos de autor y derechos conexos[14]; e) otras formas de responsabilidad y sanción: tentativa y complicidad, responsabilidad de las personas jurídicas. Además, todos los delitos deberán estar sujetos a sanciones efectivas, proporcionadas y disuasorias, incluidas penas privativas de libertad.

Sobre las normativas penales de procedimiento, se aclara que éstas deberán aplicarse no sólo a los delitos anteriormente mencionados, sino que además a cualquier otro delito cometido por medio de un sistema informático y también a la obtención de pruebas electrónicas de cualquier delito. En el Convenio de Budapest se establece como condiciones y salvaguarda, que en la aplicación de dichas normativas, los Estados deberán garantizar una adecuada protección de los derechos humanos y de las libertades fundamentales derivadas de los principales tratados internacionales sobre el tema, figurando entre ellos la privacidad, la libertad de expresión, entre otros. Otra de las cuestiones que hacen a las normativas procesales tiene que ver con la conservación rápida de datos informáticos almacenados por un tiempo determinado; la conversación y revelación parcial rápida de los datos relativos al tráfico; la orden de presentación, el

[13] El Convenio define lo que debe entenderse por sistema informático y datos informáticos. Por "sistema informático" se entenderá 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. Por "datos informáticos" se entenderá toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función.

[14] El derecho de autor se aplica a las creaciones literarias y artísticas como los libros, las obras musicales, las pinturas, las esculturas, las películas y las obras realizadas por medios tecnológicos como los programas informáticos y las bases de datos electrónicas. La finalidad de los derechos conexos, también conocidos como derechos afines al derecho de autor, es proteger los intereses legales de determinadas personas y entidades jurídicas que contribuyen a la puesta a disposición del público de obras o que hayan producido objetos que, aunque no se consideren obras en virtud de los sistemas de derecho de autor de todos los países, contengan suficiente creatividad y capacidad técnica y organizativa para merecer la concesión de un derecho de propiedad que se asimile al derecho de autor. Hasta la fecha se han venido otorgando derechos conexos a tres categorías de beneficiarios: artistas intérpretes y ejecutantes; productores de fonogramas; y organismos de radiodifusión. Organización Mundial de la Propiedad Intelectual, *En Principios básicos del derecho de autor y derechos conexos*, OMPI, 2016, en http://www.wipo.int/edocs/pubdocs/es/wipo_pub_909_2016.pdf.

registro y la confiscación de datos informáticos almacenados; la obtención en tiempo real de datos relativos al tráfico y la interceptación de datos relativos al contenido.

En cuanto a la cooperación internacional, se establece que los Estados cooperarán entre sí en materia penal a efectos de las investigaciones o los procedimientos relativos a los delitos relacionados con sistemas y datos informáticos o para obtener pruebas en formato electrónico de los delitos. También se establecen principios referidos a la extradición entre los Estados por los delitos cometidos, y principios generales relativos a la asistencia mutua a efecto de las investigaciones y procedimientos relativos a los delitos relacionados con sistemas informáticos y datos informáticos o con el fin de obtener pruebas en formato electrónico de un delito.

Finalmente, el Convenio trata del acceso transfronterizo a datos almacenados que requieren consentimiento y aquellos que no lo necesitan por ser datos accesibles al público, como así mismo contempla la creación una red 24/7 entre los Estados con el fin de garantizar una asistencia inmediata para investigaciones relativas a delitos vinculados a sistemas y datos informáticos, o para obtener las pruebas en formato electrónico de un delito.

Entre las principales prácticas de ciberdelincuencia o delitos de ingeniería social[15] que marcaron el 2017[16], se encuentran el *ransomware*[17], las infecciones de *malware* sin descargar de archivos[18], los ataques DDoS en servidores y sistemas web globales[19], el tráfico HTTPs malicioso: protocolos cifrados como señuelo[20], el *maladvertising*[21], el *phishing-spearphishing*[22], el fraude cara a cara[23], los móviles e información en las

---

[15] Es la práctica consistente en obtener información confidencial o medios de acceso a sistemas informáticos mediante el engaño.

[16] Wolters Kluwers España, *Los 10 delitos digitales que marcarán la ciberseguridad en 2017,* Especial Directivos, N° 1705, 1ª quincena, febrero 2017.

[17] Software malicioso que se utiliza para bloquear el acceso a archivos o determinadas partes del dispositivo de la víctima, con el objeto de pedir un rescate a cambio de eliminar restricciones.

[18] Técnica consistente en infectar directamente la memoria RAM de los ordenadores y dispositivos móviles, sin que el usuario tenga que recibir, abrir, o descargar ningún tipo de archivo.

[19] Los ataques de Denegación de servicio o DDos por sus siglas en inglés *(Distributed Denial of Services)*, pueden llegar a sobrecargar los servidores a través de un volumen de peticiones masivo que supera sus capacidades. Estas solicitudes de servicios son ficticias, normalmente generadas a través de robots conectados (*bots*), e impiden a los usuarios reales acceder a los contenidos de los servidores.

[20] Tráfico malicioso cifrado a través de protocolos HTTPs que encubre las acciones criminales y las hacen pasar como seguras.

[21] Modalidad que consiste en realizar una compra legítima de espacios publicitarios en sitios webs o aplicaciones conocidas como seguras, en los que se emplazan anuncios publicitarios para dirigir tráfico hacia las propias páginas maliciosas o descargar archivos que contienen *malware* u otro tipo de software dañino.

[22] El *phishing* consiste en la suplantación de la identidad de las personas o empresas para adquirir información trascendental de forma fraudulenta. El *spearphishing* es una variante realizada por medio del

nubes[24], el internet de las cosas[25] y la inteligencia artificial[26]. Conviene aclarar que mucho de los ejemplos de conductas delictivas de ingeniería social no están contemplados específicamente como delitos en los Códigos Penales de los diferentes países a nivel mundial.

2.3 Regulación jurídica de la Ciberseguridad en la Unión Europea

En lo que refiere a la protección de la ciberseguridad en la Unión Europea existen dos directivas aprobadas sobre el tema. La primera de ellas es la Directiva 2013/40/UE, relativa a los ataques contra los sistemas de información, que tiene por objeto establecer normas mínimas relativas a la definición de las infracciones penales y a las sanciones aplicables en el ámbito de los ataques contra los sistemas de información, además de facilitar la prevención de dichas infracciones y la mejora de la cooperación entre las autoridades judiciales y otras autoridades competentes.

En la presente normativa se establecen como infracciones penales las infracciones comunes de acceso ilegal a un sistema de información, de intromisión ilegal en el sistema, de intromisión ilegal en los datos y de interceptación ilegal[27]. Así mismo se establecen medidas eficaces contra la usurpación de identidad y otras infracciones relacionadas con la identidad. Para los casos graves se contemplan sanciones más severas cuando un ataque contra un sistema de información se comete en el contexto de una organización delictiva o cuando el ciberataque se realice a gran escala y afecta a un número importante de sistemas de información, en particular cuando el ataque tiene como finalidad crear una red infectada o bien afecta infraestructuras críticas.

---

correo electrónico, con la finalidad de suplantar la identidad de la persona o empresa para adquirir dicha información.

[23] Casos de estafa en que se solicita personalmente la información de manera engañosa para obtener y acceder a información digital de los usuarios. Un ejemplo es el fraude telefónico, en que los delincuentes se hacen pasar por técnicos de soporte de fabricantes informáticos para instalar programas de código malicioso en los dispositivos de los usuarios o conseguir datos de sus cuentas bancarias.

[24] Vulneración de dispositivos móviles para acceder a los datos de las personas y las empresas que se encuentran almacenados en sitios webs.

[25] Internet de las cosas (en inglés, *Internet of Things*, abreviado *IoT*) es un concepto que se refiere a la interconexión digital de objetos cotidianos con Internet.

[26] La inteligencia artificial, en forma de algoritmos programados para optimizar la toma de decisiones y ejecución de acciones, puede ser vulnerada para favorecer los intereses de los atacantes y comprometer la actividad de las empresas.

[27] Transmisiones no públicas de datos informáticos hacia, desde o dentro de un sistema de información, incluidas las emisiones electromagnéticas de un sistema de información que contenga dichos datos informáticos, intencionalmente y sin autorización, sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad.

Se menciona la importancia de contar con redes de puntos de contacto[28] efectivas en los Estados miembros, y que éstas deberán estar disponibles veinticuatro horas al día, los siete días de la semana, con la finalidad de prestar asistencia efectiva. Se subraya la cooperación entre las autoridades por un lado y el sector privado y la sociedad civil por otro, para evitar y combatir los ataques contra los sistemas de información. Finalmente, se insta a los Estados miembros a mejorar la cooperación internacional en lo relativo a la seguridad de los sistemas de información, de las redes de ordenadores y de los datos que albergan, y en los acuerdos internacionales relativos al intercambio de datos debe tomarse debidamente en consideración la seguridad de la transferencia de datos y del almacenamiento de estos.

En segundo lugar, fue aprobada la Directiva 1148/2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información de la Unión, conocida también como Directiva sobre Seguridad de las Redes y Sistemas de Información (SRI). El objetivo de la presente directiva es hacer frente y dar una respuesta efectiva a los problemas de seguridad que plantean las redes y los sistemas de información[29] de la Unión, ante el peligro que suponen las actividades ilícitas desarrolladas en internet, que afectan tanto a las estructuras críticas como a los usuarios.

Con esta finalidad, se establecen para los Estados miembros requisitos mínimos comunes en materia de desarrollo de capacidades y planificación, intercambio de información, cooperación y requisitos de seguridad para los operadores de servicios esenciales[30] y los proveedores de servicios digitales[31]. Se mencionan requisitos especiales de seguridad para combatir los ataques con mayor rapidez y eficacia, y la obligación de denunciar los ataques para las empresas que ofrezcan servicios esenciales, como ser la energía, el transporte marítimo y fluvial, el sector bancario y las infraestructuras de los mercados financieros, suministro y distribución de agua potable,

[28] Agencias estatales que han de poder prestar asistencia efectiva, facilitando así, por ejemplo, el intercambio de la información relevante disponible o prestando asesoramiento técnico o información jurídica en el marco de investigaciones o procedimientos relativos a infracciones penales relacionadas con sistemas de información y de datos asociados que impliquen al Estado miembro solicitante.

[29] Todo dispositivo o grupo de dispositivos interconectados o relacionados entre sí, en el que uno o varios de ellos realizan, mediante un programa, el tratamiento automático de datos digitales, o los datos digitales almacenados, tratados, recuperados o transmitidos para su funcionamiento, utilización, protección y mantenimiento.

[30] Entidad pública o privada que presta un servicio esencial para el mantenimiento de actividades sociales o económicas cruciales. La prestación de dicho servicio depende de las redes y sistemas de información, y un incidente tendría efectos perturbadores significativos en la prestación del servicio.

[31] Todo servicio prestado normalmente a cambio de una remuneración, a distancia, por vía electrónica y a petición individual de un destinatario de servicios.

infraestructura digital y asistencia sanitaria, los servicios de mercados en línea[32], motores de búsqueda en línea[33] y la computación en las nubes[34]. También el resto de las empresas deberán denunciar cualquier tipo de ataques a sus redes cuando los mismos puedan tener un efecto perturbador significativo[35].

Las principales obligaciones de la Directiva 1148/2016 pueden resumirse en cinco puntos. En primer lugar, establecer obligaciones para todos los Estados miembros de adoptar una estrategia nacional de seguridad de las redes y sistemas de información. Segundo, se debe crear un grupo de cooperación para apoyar y facilitar la cooperación estratégica y el intercambio de información entre los Estados miembros y desarrollar confianza y seguridad entre ellos.

La tercera cuestión que se contempla es crear una red de quipos de respuestas a incidentes de seguridad informática (red CSIRT[36]) con el fin de contribuir al desarrollo de la confianza y seguridad entre los Estados miembros y promover una cooperación operativa rápida y eficaz. En cuarto lugar, establecer requisitos de seguridad y notificación para los operadores de servicios esenciales y para los proveedores de servicios digitales, y en quinto y último lugar, obligar a los Estados que designen autoridades nacionales competentes, puntos de contacto únicos y CSIRT con funciones relacionadas a la seguridad de las redes y sistemas de información.

Con miras a fortalecer el mercado único digital en la Unión Europea y mejorar su respuesta a los ataques informáticos, a finales del 2017 el Consejo Europeo solicitó la adopción de una reforma para reforzar sus normativas sobre ciberseguridad, destacándose la creación del Equipo de Respuestas a Emergencias Informáticas (CERT-UE), de carácter permanente. Además, propuso la introducción de regímenes de certificación a escala de la Unión Europea para los productos, servicios y procesos de las TIC. Otras propuestas adoptadas tienen que ver con la adopción de una Directiva

---

[32] Servicio digital que permite a los consumidores o a los comerciantes celebrar contratos de compraventa o de servicios en línea con comerciantes, ya sea en el sitio web del mercado en línea o en un sitio web de un comerciante que utilice servicios informáticos proporcionados por el mercado en línea.

[33] Servicio digital que permite a los usuarios hacer búsquedas de, en principio, todos los sitios webs o de sitios web en una lengua en concreto mediante una consulta sobre un tema cualquiera en forma de palabra clave, frase u otro tipo de entrada, y que en respuesta muestra enlaces en los que puede encontrarse información relacionada con el contenido solicitado.

[34] Servicio digital que hace posible el acceso a un conjunto modulable y elástico de recursos informáticos que se pueden compartir.

[35] Son ataques a las redes o incidentes en los que se tienen en cuenta factores como el número de usuarios que se ven afectados, la repercusión en términos de grado y duración, en las actividades económicas o sociales o en la seguridad pública, la extensión geográfica con respecto a la zona que podría verse afectada por un incidente, existencia de alternativas para la prestación del servicio, entre otros.

[36] Por sus siglas en inglés de *Computer Seucurity Incident Response Team.*

contra el fraude y la falsificación de los medios de pagos distintos del efectivo[37] y el refuerzo de la estabilidad mundial a través de la cooperación internacional[38].

Entre otras normativas vinculadas a regular aspectos concretos de la ciberseguridad en la Unión Europea tenemos el nuevo Reglamento Europeo de Protección de Datos 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos); el protocolo relacionado a la transferencia internacional de datos conocido como *Privacy Shield*, y la Directiva sobre Comercio Electrónico 31/2000, normativas que posteriormente serán analizadas en el siguiente capítulo.

2.4 Regulación jurídica de la Ciberseguridad en los Estados Unidos

En el año 2002 fue sancionada la Ley Federal de Gestión de la Seguridad de la Información (FISMA, *Federal Information Security Management Act*), conocida también como Ley *E-Government,* con la finalidad de que cada institución pública o agencia federal de los Estados Unidos pueda desarrollar, documentar e implementar programas que aumenten la seguridad de la información y de los sistemas de información que respaldan las operaciones y los activos de la agencia, incluidos los provistos o administrados por otra agencia, contratista u otra fuente.

Con esta normativa y en lo referente a la ciberseguridad, se buscó que los organismos públicos implementen políticas y procedimientos para reducir de manera rentable los riesgos de seguridad de la tecnología de la información a un nivel aceptable. Según FISMA, el término seguridad de la información significa proteger la información y los sistemas de información del acceso no autorizado, uso, divulgación, interrupción, modificación o destrucción a fin de proporcionar integridad, confidencialidad y disponibilidad. Posteriormente, en el 2015 fue sancionada en los Estados Unidos la Ley de Intercambio de Información de Ciberseguridad (CISA, *Cybersecurity Information Sharing Act*) con el objetivo de mejorar la seguridad cibernética en los Estados Unidos a través de un mayor intercambio de información sobre las amenazas de ciberseguridad y

[37] El 13 de enero del 2018 entró en vigor la nueva Directiva de Servicios de Pagos de la Unión Europea conocida como PSD2 (*Payment Service Directive 2*) que busca facilitar y dotar de mayor seguridad al sector financiero en los servicios de pagos digitales y ofrecer además un servicio bancario adaptado a las nuevas tecnologías.

[38] Los países de la Unión Europea podrán celebrar acuerdos internacionales con terceros países u organizaciones internacionales que hagan posible y organicen su participación en algunas actividades del grupo de cooperación. En tales acuerdos se tendrá en cuenta la necesidad de garantizar una protección de datos adecuada.

otros afines. La ley permite el intercambio de información sobre el tráfico de Internet[39] entre el gobierno de los Estados Unidos y el sector privado.

Las principales disposiciones de la referida ley facilitan que tanto las agencias estatales como las empresas privadas compartan información personal con el gobierno, especialmente en los casos de indicadores de amenazas de ciberseguridad[40]. A pesar de que no se establece la obligatoriedad en el intercambio de información y manejo de incidentes por parte de las empresas privadas -a diferencia de los organismos estatales- la ley crea un sistema para que las agencias federales reciban información de amenazas de parte del sector privado. Los incidentes de ataques de seguridad reportados, son revisados por dos agencias federales separadas: el Departamento de Seguridad Nacional (NSA) y el Equipo de Preparación para Emergencias Informáticas (US-CERTg).

Con respecto a la privacidad, la ley incluye disposiciones para evitar compartir datos que se sabe que son personalmente identificables e irrelevantes para la ciberseguridad. Cualquier información personal que no se elimine durante el procedimiento de uso compartido se puede usar de varias maneras. Estos indicadores compartidos de amenaza cibernética se pueden utilizar para perseguir delitos informáticos, pero también se pueden usar como evidencia de otros delitos que involucran fuerza física.

Otras normativas federales sobre ciberseguridad en los Estados Unidos se refieren a industrias o sectores específicos. Entre ellos se encuentran la Ley de Responsabilidad y Portabilidad del Seguro de Salud de 1996, la Ley de Modernización de Servicios Financieros de 1999 y la Ley de Seguridad Nacional del 2002, todas estas referidas al establecimiento de estándares nacionales para la protección de los sistemas e información referida a las transacciones electrónicas de los servicios de salud, instituciones financieras y agencias federales.

2.5 Regulación de la Ciberseguridad en América

En la Asamblea General de la Organización de los Estados Americanos (OEA) en 2004, los Estados miembros aprobaron la Estrategia Interamericana Integral para Combatir las

[39] También conocido como tráfico web o tráfico online, se refiere a la cantidad de datos enviados y recibidos por los visitantes de un sitio web.

[40] Información que es necesaria para describir o identificar: reconocimiento malicioso; un método para burlar un control de seguridad o la explotación de una vulnerabilidad de seguridad; una vulnerabilidad de seguridad; un método para hacer que un usuario con acceso legítimo a un sistema de información o información que esté almacenada, procesada o en tránsito por un sistema de información permita involuntariamente burlar un control de seguridad o explotación de una vulnerabilidad de seguridad; comando y control cibernético malicioso; el daño real o potencial causado por un incidente, incluida una descripción de la información exfiltrada como resultado de una amenaza particular de ciberseguridad; cualquier otro atributo de una amenaza de ciberseguridad, si la divulgación de dicho atributo no está prohibida por la ley; o cualquier combinación de los mismos.

Amenazas a la Seguridad Cibernética, por medio de la resolución AG/RES. 2004 (XXXIV-O/04), proporcionando así el mandato que permite a la Secretaría del Comité Interamericano contra el Terrorismo (CICTE) trabajar en asuntos de Seguridad Cibernética. La Secretaría del CICTE emplea un enfoque integral en la construcción de capacidades de seguridad cibernética entre los estados miembros, reconociendo que la responsabilidad nacional y regional para la seguridad cibernética cae sobre una amplia gama de entidades tanto del sector público como el privado, los cuales trabajan en aspectos políticos y técnicos para asegurar el ciberespacio.

Entre los principales objetivos de la Secretaría, se encuentran el establecimiento de grupos nacionales de "alerta, vigilancia y prevención", también conocidos como Equipos de Respuesta a Incidentes (CSIRT) en cada país; crear una red de alerta hemisférica que proporciona formación técnica a personal que trabaja en la seguridad cibernética para los gobiernos de las Américas; promover el desarrollo de Estrategias Nacionales sobre Seguridad Cibernética y fomentar el desarrollo de una cultura que permita el fortalecimiento de la Seguridad Cibernética en el Hemisferio[41]. Entre los principales documentos de la OEA divulgados sobre ciberseguridad se encuentran la "Declaración sobre el Fortalecimiento de la Seguridad Cibernética en las Américas[42]" del 2004, que posteriormente fue complementado por la "Estrategia Interamericana Integral para Combatir las Amenazas a la Seguridad Cibernética[43]" en el 2012.

A nivel MERCOSUR, desde el año 2014 se cuenta con la Reunión de Autoridades sobre Privacidad y Seguridad de la Información e Infraestructura Tecnológica del MERCOSUR (RAPRISIT), como órgano auxiliar encargado de proponer políticas e iniciativas comunes en el área de la seguridad cibernética y la privacidad. Tuvieron hasta el momento dos reuniones ordinarias, y en la última reunión del 9/10/2015 habían propuesto un párrafo para el Comunicado Conjunto de Presidentes del MERCOSUR y Estados Asociados[44].

---

[41] https://www.sites.oas.org/cyber/Es/Paginas/default.aspx

[42] Esta declaración significó para los Estados miembros de la OEA el reconocimiento de que combatir los delitos cibernéticos y fortalecer la resiliencia cibernética, eran cuestiones imperativas para el desarrollo económico y social, la gobernanza democrática, la seguridad nacional y la de los ciudadanos.

[43] La estrategia reconoce la necesidad de que todos los participantes en las redes y sistemas de información sean conscientes de sus funciones y responsabilidades con respecto a la seguridad a fin de crear una cultura de seguridad cibernética, como así también se reconoce un marco eficaz para la protección de las redes y sistemas de información que integran la internet, y la manera de responder a incidentes y recuperarse de los mismos.

[44] "Reconocer la importancia de las funciones de la RAPRISIT para la proposición de políticas e iniciativas comunes en el área de seguridad cibernética, la privacidad, la protección de los datos personales, la confianza en el uso de internet, la interconexión de infraestructuras, la prevención y el

2.6 Regulación jurídica de la Ciberseguridad en el Paraguay

En el Paraguay -al igual que en la mayoría de los países a nivel mundial- no existe una regulación específica que trate propiamente la ciberseguridad en un solo cuerpo normativo[45], sino que se encuentra diseminada en varias normativas que tratan diversos aspectos vinculados al tema. Sin embargo, podemos mencionar que la ley N° 4.989/2013 Que crea el marco de aplicación de las Tecnologías de la Información y Comunicación en el sector público y crea la Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs), es la normativa que en materia de ciberseguridad atribuye a la SENACTICS la tarea de establecer y gestionar las políticas de protección de la información personal y gubernamental, y cultivar los conocimientos sobre la industria de seguridad de la información, para lo cual deberá establecer un sistema de organización de seguridad, proponer una política de seguridad a nivel nacional, y establecer un plan de integración de protección de la información[46]".

El Decreto N° 7052/2017 del Poder Ejecutivo aprobó el Plan Nacional de Ciberseguridad, elaborado por la Secretaría Nacional de Tecnologías de Información y Comunicación (SENATICS), en coordinación con el Ministerio de Relaciones Exteriores (MRE) y con el apoyo de la Organización de los Estados Americanos (OEA). El Plan Nacional de Ciberseguridad es un documento estratégico que sirve como fundamento para la coordinación de las políticas públicas de ciberseguridad, integrando a todos los sectores en el desarrollo de las tecnologías de la información y comunicación (TIC) en un ambiente cibernético confiable y resiliente. Según se establece "este Plan Nacional busca avanzar con la ciberseguridad en Paraguay de modo a fomentar el uso confiable de las TIC en el país, impulsando un cambio cultural en la sociedad para el uso seguro del ciberespacio, así como el progreso y la innovación en el país, fomentado

---

combate al cibercrimen mediante estrategias y políticas de ciberseguridad, promoviendo la coordinación local y regional respetando las particularidades de los Estados miembros. Asimismo, ratifican la necesidad de fomentar el desarrollo de espacios de diálogo y/o mecanismos nacionales de múltiples partes interesadas en la gobernanza de internet, incluidos gobiernos, sector privado, sociedad civil, comunidad técnica y académica. En tal sentido, reafirman el compromiso de promover una internet libre, abierta, interoperable, neutral y para todos los habitantes". http://gd.mercosur.int/SAM%5CGestDoc%5Cpubweb.nsf/436C650CF20409AD0325824A00623C8B/$File/RAPRISIT_2015_ACTA02_ANE03_ES_PropParrafoComunicado.pdf

[45] España por ejemplo cuenta con un Código de Derecho a la Ciberseguridad, consistente en una recopilación de toda la normativa española vinculada a la ciberseguridad y dividida por ejes temáticos. Así, el Código se divide en: Constitución Española, normativas de seguridad nacional, infraestructuras críticas, normativas de seguridad, equipo de respuesta a incidentes de seguridad, telecomunicaciones y usuarios, ciberdelincuencia, protección de datos y relación con la administración.

[46] Art. 12, Inc. g de la ley N° 4989/2013. Por su parte, el Inc. h dispone "diseñar e implementar estándares, mecanismos y medidas tecnológicas de seguridad para el adecuado funcionamiento de los programas y servicios de acceso electrónico para el ciudadano".

un entorno económico favorable al crecimiento, desarrollo y competitividad de las nuevas tecnologías[47]".

El documento en cuestión está compuesto por un diagnóstico sobre la ciberseguridad en el país, y "tiene como principios orientadores para la formulación e implementación de cualquier política pública de ciberseguridad en Paraguay, el de proporcionalidad, coordinación de esfuerzos y uso eficiente de recursos escasos, responsabilidad compartida, desarrollo e innovación, cooperación internacional y monitoreo y evaluación. Asimismo, se centra en siete ejes de acción que consisten en: 1) Sensibilización y cultura; 2) Investigación, desarrollo e innovación; 3) Protección de infraestructuras críticas; 4) Capacidad de respuesta ante incidentes cibernéticos; 5) Capacidad de investigación y Persecución de la Ciberdelincuencia; 6) Administración Pública y 7) Sistema Nacional de Ciberseguridad[48]".

Toda la gestión de incidentes y vulnerabilidades cibernéticas es llevada a cabo a través del Centro de Respuestas a Incidentes Cibernéticos del Paraguay (CERT-PY), que se encuentra bajo la Dirección General de Políticas y Desarrollo de TIC de la SENATICs, creado el 30 de noviembre del 2012 con el objetivo principal de actuar como coordinador central para las notificaciones de incidentes de seguridad en Paraguay, dando el apoyo necesario para dar respuesta a estos incidentes, haciendo que las partes afectadas e involucradas entren en contacto para la solución de los mismos. Otro objetivo importante, además del tratamiento de los incidentes, es el de promocionar la concienciación sobre los problemas de seguridad, del análisis de los niveles actuales, las tendencias y la relación entre los diferentes incidentes que ocurran dentro del país[49].

Para la coordinación y ejecución efectiva del Plan Nacional de Ciberseguridad se establece el Sistema Nacional de Ciberseguridad, conformada por un Coordinador Nacional como máximo, responsable de monitorear y evaluar la implementación de los objetivos y las líneas de acción, y por una Comisión Nacional de Ciberseguridad, principal organismo ejecutor de la política nacional sobre ciberseguridad e integrado por varias instituciones públicas. A su vez, se resalta en el Plan la necesidad de fomentar la cooperación entre el sector público y privado, la academia y la sociedad civil para la consecución de las líneas de acción.

---

[47] Plan Nacional de Ciberseguridad. Retos, Roles y Desafíos, Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs), Asunción, 2017, 22.

[48] Considerando del Decreto N° 11.624/2013 por el cual se reglamenta la Ley N° 4989/13.

[49] En https://www.cert.gov.py/index.php/certpy

En cuanto a la regulación de la ciberdelincuencia en el Paraguay, en el año 2011 fue aprobada la ley N° 4439/2011 que modifica y amplía artículos del Código Penal, mejor conocida como Ley contra los Delitos Informáticos, modificando y adaptando nuestra legislación penal a los estándares mínimos, establecidos en el Convenio de Budapest sobre Ciberdelincuencia. La ley modificó tres artículos del Código Penal, siendo estos los relativos a pornografía relativa a niños y adolescentes[50], sabotaje de sistemas informáticos[51] y estafa mediante sistemas informáticos[52], e introdujo seis nuevos artículos relativos al acceso indebido de datos[53], interceptación de datos[54], preparación

[50] "Art. 140.-Pornografía relativa a niños y adolescentes. 1° El que: 1. produjere publicaciones, en el sentido del Artículo 14, inciso 3°, que representen actos sexuales con participación de personas menores de dieciocho años de edad o la exhibición de sus partes genitales; 2. organizara, financiara o promocionara espectáculos, públicos o privados, en los que participe una persona menor de dieciocho años en la realización de actos sexuales, o; 3. distribuyera, importara, exportara, ofertara, canjeara, exhibiera, difundiera, promocionara o financiara la producción o reproducción de publicaciones en sentido del numeral 1, será castigado con pena privativa de libertad de hasta cinco años o multa. 2° El que reprodujera publicaciones según el numeral 1 del inciso 1°, será castigado con pena privativa de libertad de hasta tres años o multa. 3° La pena de los incisos anteriores podrá ser aumentada hasta diez años cuando: 1. las publicaciones y espectáculos en el sentido de los incisos 1° y 2° se refieran a menores de catorce años o se dé acceso a los menores de dicha edad a publicaciones y espectáculos, en sentido de los incisos citados; 2. el autor tuviera la patria potestad, deber de guarda o tutela del niño o adolescente, o se le hubiere confiado la educación o cuidado del mismo; 3. el autor operara en connivencia con personas a quienes competa un deber de educación, guarda o tutela respecto del niño o adolescente; 4. el autor hubiere procedido, respecto del niño o adolescente, con violencia, fuerza, amenaza, coacción, engaño, recompensa o promesa remuneratoria de cualquier especie; o 5.el autor actuara comercialmente o como miembro de una banda dedicada a la realización reiterada de los hechos punibles señalados. 4° El que obtuviera la posesión de publicaciones en el sentido de los incisos 1° y 3°, será castigado con pena privativa de libertad de hasta tres años o con multa. 5°Se aplicará, en lo pertinente, también lo dispuesto en los Artículos 57 y 94."

[51] "Art. 175.- Sabotaje de sistemas informáticos. 1°El que obstaculizara un procesamiento de datos de un particular, de una empresa, asociación o de una entidad de la administración pública, mediante: 1. un hecho punible según el Artículo 174, inciso 1°; o 2. la destrucción, inutilización, sustracción o alteración de una instalación de procesamiento de datos, de una unidad de almacenamiento o de otra de sus partes componentes indispensable, será castigado con pena privativa de libertad de hasta cinco años o con multa. 2° En estos casos será castigada también la tentativa."

[52] "Artículo 146 c.- Interceptación de datos. El que, sin autorización y utilizando medios técnicos: 1°obtuviere para sí o para un tercero, datos en sentido del Artículo 146 b, inciso 2°, no destinados para él; 2°diera a otro una transferencia no pública de datos; o 3° transfiriera la radiación electromagnética de un equipo de procesamiento de datos, será castigado con pena privativa de libertad de hasta dos años o multa, salvo que el hecho sea sancionado por otra disposición con una pena mayor."

"Artículo 146 d.- Preparación de acceso indebido e interceptación de datos. 1° El que prepare un hecho punible según el Artículo 146 b o el Artículo 146 c produciendo, difundiendo o haciendo accesible de otra manera a terceros: 1.las claves de acceso u otros códigos de seguridad, que permitan el acceso a datos en sentido del Artículo 146 b, inciso 2°; o 2.los programas de computación destinados a la realización de tal hecho, será castigado con pena privativa de libertad de hasta un año o multa. 2° Se aplicará, en lo pertinente, lo previsto en el Artículo 266, incisos 2° y 3°."

[53] "Artículo 146 b.- Acceso indebido a datos. 1°El que sin autorización y violando sistemas de seguridad obtuviere para sí o para terceros, el acceso a datos no destinados a él y especialmente protegidos contra el acceso no autorizado, será castigado con pena privativa de libertad de hasta tres años o multa. 2° Como datos en sentido del inciso 1°, se entenderán solo aquellos, que se almacenan o transmiten electrónicamente, magnéticamente o de otra manera no inmediatamente visible."

[54] "Artículo 146 c.- Interceptación de datos. El que, sin autorización y utilizando medios técnicos: 1°obtuviere para sí o para un tercero, datos en sentido del Artículo 146 b, inciso 2°, no destinados para él; 2°diera a otro una transferencia no pública de datos; o 3° transfiriera la radiación electromagnética de

de acceso indebido e interceptación de datos[55], acceso indebido a sistemas informáticos[56], a la instancia[57], y a la falsificación de la tarjetas de débito o de crédito y otros medios electrónicos de pagos[58]. En lo que respecta a las instituciones especializadas para combate a la ciberdelincuencia, se cuenta con la Unidad Especializada de Delitos Informáticos de la Fiscalía General del Estado y la División Especializada contra Delitos Informáticos de la Policía Nacional. En cuanto a la seguridad y fomento de las TICS a nivel país, contamos especialmente con la regulación de la firma digital[59] y con una ley sobre comercio electrónico[60]. Por medio del Decreto N° 6234/2016 por el cual se declara de interés nacional la aplicación y el uso de las TICs en la gestión pública, se ordena a las instituciones dependientes del Poder Ejecutivo contar con unidades especializadas en TIC con la finalidad de promover la implementación, acrecentamiento y acceso a la infraestructura y a las tecnologías de la

---

un equipo de procesamiento de datos, será castigado con pena privativa de libertad de hasta dos años o multa, salvo que el hecho sea sancionado por otra disposición con una pena mayor."

[55] "Artículo 146 d.- Preparación de acceso indebido e interceptación de datos. 1° El que prepare un hecho punible según el Artículo 146 b o el Artículo 146 c produciendo, difundiendo o haciendo accesible de otra manera a terceros: 1. las claves de acceso u otros códigos de seguridad, que permitan el acceso a datos en sentido del Artículo 146 b, inciso 2°; o 2. los programas de computación destinados a la realización de tal hecho, será castigado con pena privativa de libertad de hasta un año o multa. 2° Se aplicará, en lo pertinente, lo previsto en el Artículo 266, incisos 2° y 3°."

[56] "Artículo 174 b.- Acceso indebido a sistemas informáticos. 1° El que accediere a un sistema informático o a sus componentes, utilizando su identidad o una ajena; o excediendo una autorización, será castigado con pena privativa de libertad de hasta tres años o multa. 2° Se entenderá como sistema informático a todo dispositivo aislado o al conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus componentes, sea el tratamiento de datos por medio de un programa informático."

[57] "Artículo 175 b.- Instancia. En los casos de los Artículos 174 y 175, la persecución penal dependerá de la instancia de la víctima; salvo que la protección del interés público requiera la persecución de oficio."

[58] "Artículo 248 b.- Falsificación de tarjetas de débito o de crédito y otros medios electrónicos de pago. 1° El que, con la intención de inducir en las relaciones jurídicas al error o de facilitar la inducción a tal error: 1. falsificare o alterare una tarjeta de crédito o débito u otro medio electrónico de pago; o 2. adquiera para sí o para un tercero, ofreciere, entregare a otro o utilizare tales tarjetas o medios electrónicos, será castigado con pena privativa de libertad de hasta cinco años o con multa. 2° Se castigará también la tentativa. 3° Cuando el autor actuara comercialmente o como miembro de una organización criminal dedicada a la realización de los hechos punibles señalados, la pena privativa de libertad podrá ser aumentada hasta diez años. 4° Tarjetas de crédito, en sentido del inciso 1°, son aquellas que han sido emitidas por una entidad de crédito o de servicios financieros para su uso en dicho tipo de transacciones y que, por su configuración o codificación, son especialmente protegidas contra su falsificación. 5°Medios electrónicos de pago en el sentido del inciso 1°, son aquellos instrumentos o dispositivos que actúan como dinero electrónico, permitiendo al titular efectuar transferencias de fondos, retirar dinero en efectivo, pagar en entidades comerciales y acceder a los fondos de una cuenta."

[59] Ley N° 4017/2010 De Validez jurídica de la firma electrónica, la firma digital, los mensajes de datos y el expediente electrónico. El art. 2 establece que la firma digital es "una firma electrónica certificada por un prestador acreditado, que ha sido creada usando medios que el titular mantiene bajo su exclusivo control, de manera que vale únicamente al mismo y a los datos a lo que se refiere, permitiendo la detección posterior de cualquier modificación, verificando la identidad del titular e impidiendo que desconozca la integridad del documento y su autoría".

[60] Ley N° 4868/2013.

información y comunicación, bajo supervisión directa de la máxima autoridad de cada institución.

La Ley N° 4868/2013 de Comercio Electrónico contiene una disposición por la cual se obliga a los proveedores en la prestación de los servicios de acceso a internet a informar a sus clientes de forma permanente, fácil, directa y gratuita, sobre los diferentes medios de carácter técnico que aumenten los niveles de la seguridad de la información y permitan, entre otras cosas, la protección frente a virus informáticos y programas espía, y la restricción de los correos electrónicos no solicitados; así como también a informar sobre las herramientas existentes para el filtrado y restricción del acceso a determinados contenidos y servicios no deseados en internet o que puedan resultar nocivos para la niñez y la adolescencia[61].

Finalmente, y para concluir el presente capítulo, haremos un recuento de las principales normativas vigentes vinculadas a la ciberseguridad en el Paraguay. Éstas son: Ley N° 642/1995 de Telecomunicaciones que crea la Comisión Nacional de Telecomunicaciones (CONATEL); Ley N° 1337/1999 De Defensa Nacional y Seguridad Interna; Ley Nº 1.582/2000 Que aprueba el Tratado de la Organización Mundial de la Propiedad Intelectual (OMPI) sobre Derecho de Autor; Ley Nº 1.583/2000 Que aprueba el Tratado de la Organización Mundial de la Propiedad Intelectual (OMPI) sobre Interpretación o Ejecución y Fonogramas; Ley N° 4868/2013 de Comercio Electrónico; Ley N° 4439/2011 Que modifica y amplía varios artículos del Código Penal referentes a los delitos informáticos; Ley N° 4989/2013 Que crea el marco de aplicación de las tecnologías de la información y comunicación en el sector público y crea la Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs); Ley N° 5653/16 De Protección de Niños, Niñas y Adolescentes contra contenidos nocivos en internet y la Ley N° 5994/17 que ratifica el Convenio de Budapest sobre Ciberdelincuencia.

3. Conclusiones

Luego de analizar las diferentes definiciones del término ciberseguridad -tanto en su sentido amplio como restringido- y constatar que no existe una definición legal sobre la

[61] Art. 9 inc. a) y b) de la ley 4868/2013. Se menciona que esta obligación de información se tendrá por cumplida si el correspondiente proveedor incluye la información exigida en su página o sitio principal de Internet. Además, el inc. c) menciona "suspender el acceso a un contenido o servicio cuando un órgano competente, en ejercicio de las competencias que legalmente tenga atribuidas, requiera que se interrumpa la prestación de un servicio o que se retire algún contenido que vulnere lo dispuesto en el Artículo 6°".

misma, hemos visto que la ciberseguridad se refiere esencialmente a la protección y salvaguarda de las infraestructuras y los datos almacenados en ellas, que poseen un valor para las organizaciones y los usuarios, y se encuentran expuestas a riesgos o amenazas debido a su tratamiento digital, especialmente a través de internet. En consecuencia, tanto los usuarios como las organizaciones –incluido el propio Estado- deben establecer mecanismos que comprendan aplicaciones, servicios y demás gestión de los activos con el fin de resguardar la información en el manejo del ciberespacio.

A nivel internacional, la ciberdelincuencia constituye uno de los aspectos más importantes vinculados a la ciberseguridad, siendo el Convenio de Budapest el principal tratado internacional para combatirla. El mismo tiene por objetivo aplicar una política penal común encaminada a la protección de la sociedad contra el cibercrimen, especialmente mediante la adopción de una legislación adecuada y el fomento de la cooperación internacional. A pesar de que nuestro país ratificó dicho instrumento internacional, muchos otros países aún no contemplan las principales prácticas para combatir la ciberdelincuencia en sus respectivas legislaciones a nivel mundial.

La Unión Europea se erige como modelo en lo que se refiere a la protección de la ciberseguridad a través de dos directivas. En una de ellas se establecen normas mínimas relativas a la definición de las infracciones penales y a las sanciones aplicables en el ámbito de los ataques contra los sistemas de información, facilitando la prevención de dichas infracciones y la mejora de la cooperación entre las autoridades, y en otra, se hace frente a los problemas de seguridad que plantean las redes y los sistemas de información ante el peligro que supone las actividades ilícitas desarrolladas en internet que afectan tanto a las estructuras críticas como a los usuarios.

En el caso de los Estados Unidos, se establecieron normativas sobre ciberseguridad dirigidas a los organismos públicos con la finalidad de implementar políticas y procedimientos que permitan reducir los riesgos de seguridad de la tecnología de la información a un nivel aceptable, además del intercambio de información sobre el tráfico de internet entre el gobierno y el sector privado para combatir las amenazas de ciberseguridad. Todo esto, complementado con otras normativas federales sobre ciberseguridad referidas a industrias o sectores específicos, como los servicios de salud, instituciones financieras y agencias federales.

La regulación de la ciberseguridad en América se da principalmente a través de la Secretaría del Comité Interamericano contra el Terrorismo (CICTE) en asuntos de seguridad cibernética, de la Organización de los Estados Americanos (OEA). La

Secretaría del CICTE se encarga de la construcción de capacidades de seguridad cibernética entre los estados miembros, trabajando tanto con el sector público como privado, en aspectos políticos y técnicos para asegurar el ciberespacio. A nivel MERCOSUR se cuenta con la Reunión de Autoridades sobre Privacidad y Seguridad de la Información e Infraestructura Tecnológica (RAPRISIT), como órgano auxiliar encargado de proponer políticas e iniciativas comunes en el área de la seguridad cibernética y la privacidad.

En lo que se refiere a Paraguay, como bien habíamos mencionado, no existe una regulación específica que trate propiamente la ciberseguridad en un solo cuerpo normativo, sino que esta se encuentra diseminada en varias normativas que tratan diversos aspectos vinculados al tema. Se destacan el Plan Nacional de Ciberseguridad, elaborado por la Secretaría Nacional de Tecnologías de Información y Comunicación (SENATICS), la ley contra los Delitos Informáticos, la firma digital, la ley de Comercio Electrónico, la aplicación y el uso de las TICs en la gestión pública, entre muchas otras.