El Ciberdelito, desafíos para la ley penal y civil. Marco jurídico nacional y comparado

Cybercrime, challenges for criminal and civil law. National and comparative legal framework

Marcelo David Benítez Vera[1]

Estudiante de Derecho de la Facultad de Ciencias Jurídicas, Políticas y Sociales de la Universidad Autónoma de Asunción (UAA). Seleccionado como Embajador para representar a la UAA y al Paraguay en el South American Business (SABF).

RESUMEN

Una consecuencia del crecimiento exponencial de la popularización de la tecnología de la información y la consiguiente migración de la actividad humana, incluida la actividadilícita, al ciberespacio está desafiando la eficacia de nuestros métodos tradicionales de aplicación de la ley. En este artículo realizaremos un breve recorrido por las distintas aristasque conforman el fenómeno del internet que cada vez está teniendo más cabida en nuestro día a día y que hoy, en la manera en que está siendo utilizada sin una regulación clara,puede amenazar la seguridad de nuestros datos privados y patrimonios e inclusive bienestar físico y psicológico.

Palabras clave: Ciberdelito, ciberespacio, cibercrimen.

ABSTRACT

A consequence of the exponential growth in the popularization of information technology and the consequent migration of human activity, including illicit activity, to cyberspace is challenging the effectiveness of our traditional methods of law enforcement. In this article we will make a brief tour of the different edges that make up the internet phenomenon that is having more and more room on a day-to-day basis and that today, in the way it is being used without clear regulation, can threaten security. of our private data and assets and even physical and psychological well-being.

Keywords: Cybercrime, cyberspace.

[1] BENÍTEZ VERA, Marcelo David. Estudiante de Derecho de la Facultad de Ciencias Jurídicas, Políticas y Sociales de la Universidad Autónoma de Asunción (UAA). Seleccionado como Embajador para representar a la UAA y al Paraguay en el South American Business (SABF).

Introducción

En las últimas décadas hemos observado desde el punto de vista social y jurídico el avance de la tecnología con sus innovaciones, especialmente en el área informática, y el impacto de la misma en el día a día de la sociedad. Estas herramientas hoy son fundamentales para comunicarnos con nuestros pares de manera social y comercial.

El ritmo con el que crece internet aún sigue creciendo vertiginosamente, la red funciona como un gran globalizador que nos une con otras personas sin importar suubicación geográfica.

A la fecha de redacción de este artículo podemos observar más de 1.964.814.295 sitios web en la red, inclusive el lector de este artículo muy posiblemente sea propietario de uno de estos sitios ante la facilidad de acceso que otorga poder adquirir un dominio que permita la creación de una página web. Actualmente aproximadamente 4.660.000.000 de personas tienen conexión a internet, lo que representa al 59,5% de la población. Estos números nos demuestran la popularización del acceso a datos y a la interconexión con otrosusuarios. Pero a medida que el uso de internet se ha masificado, ha aumentado su uso inadecuado e ilegítimo (Digital 2022 Global Overview Report, enero 2022).

Con la masificación de la red le ha acompañado el aumento de los comportamientos ilícitos dentro de la misma, donde podemos incluir a la piratería informática, el acceso sin autorización información privada, el fraude a través de la red, el sabotaje informático y la pornografía infantil. Esto ha ampliado el campo de estudio concerniente a los juristas introduciendo nuevos retos a los que debemos enfrentarnos.

El ciberespacio

Tim Jordán escribió al respecto lo siguiente:

> El ciberespacio es un entorno artificial, no físico, creado por equipos de cómputo unidos para interoperar en una red (Jordán, 1999).

Desde el nacimiento de Internet, el ciberespacio ha pasado de ser una plataforma desconocida, utilizada casi exclusivamente por académicos y tecnólogos, a una red de

infraestructura que compite con la importancia de la electricidad o la educación, y está presente en casi todos los aspectos de nuestro día a día. A medida que el uso de internet se ha extendido, ha aumentado el riesgo de su uso inadecuado.

La neutralidad, la popularidad y el anonimato son caracteres distintivos y definitorios del ciberespacio, estos elementos son un caldo de cultivo para atraer conductas delictuosas que puedan afectar el armónico desarrollo de la sociedad, estas conductas son denominadas delitos informáticos.

Julio Téllez-Valdés (2007) define al delito informático como "actitud contraria a los intereses de las personas en que se tiene a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tiene a las computadoras como instrumento o fin (concepto típico)".

Se puede decir que los perpetradores de estos delitos son conocedores de tecnología con capacidades para vulnerar sistemas informáticos a través de distintas técnicas que iremos estudiando más adelante y no solo con fines económicos, sino que puede deberse a otros intereses como la curiosidad, las cuestiones ideológicas y filantrópicas o el simple interés de causar daño a otros individuos.

Los ciberdelitos y su diferencia con el delito en el "mundo real"

La peculiaridad del ciberdelito radica en que debe realizarse a través del ciberespacio, por lo que la posibilidad de ingresar a ese espacio es una condición necesaria para su categorización. Este es un fenómeno delictivo que no es necesariamente territorial, ni puede caracterizarse por parámetros clásicos de orden general que dependen del nivel cultural de una zona específica y no responde a parámetros personalizados tradicionales sobre perpetradores y víctimas y su mayor o menor amenaza o riesgo debido al anonimato yla naturaleza global, cualquiera puede ser perpetrador o, en última instancia, víctima.Debido a su migración en el tiempo y el espacio, el tiempo y lugar de un delito o acto delictivo es impredecible e incontrolable.

Conforme a las Resoluciones Nº 3459/10 y 4408/11, los tipos penales que se pueden enmarcar como ciberdelitos en nuestro país son: Acceso indebido a datos, interceptación, preparación al acceso indebido a datos, alteración de datos, acceso indebido a sistemas

informáticos, sabotaje a sistemas informáticos, alteración de datos relevantes, falsificación de tarjetas de crédito y débito y estafa mediante sistemas informáticos.

Estos ciberdelitos se pueden lograr mediante incidentes informáticos entre los cuales podemos destacar según el informe de seguridad del CERT Centro de Respuestas a Incidentes Cibernéticos en 2020:

Phishing: Consiste en páginas web o formularios falsos, que buscan personificar alguna organización de confianza para que las víctimas ingresen sus credenciales y/o información personal en ella, y ésta sean obtenidas así por el atacante.

Software malicioso (Malware): Son porciones de código malicioso que ejecuta acciones maliciosas en el sistema que es instalado; se puede tratar de un virus, troyano, gusano, script, ransomware, etc. pudiendo tener varios objetivos: robo de información, envío de spam, keylogger, control remoto del equipo infectado, entre muchas otras.

Correo no deseado malicioso (Spam/Scam): correos electrónicos maliciosos que son enviados desde cuentas de correo o servidores de correo comprometidos, o máquinas infectadas que forman parte de una spam-botnet. Los correos maliciosos pueden distribuir malware, campañas de phishing o pueden ser simplemente engaños o estafas (estafa nigeriana, hoax u otro tipo de mensajes engañosos).

Acceso indebido a cuentas, sistemas o sus datos: esta categoría describe un evento en el cual un atacante logra acceder de manera no autorizada a alguna cuenta o a algún conjunto de datos, a través de alguna técnica cibernética (explotación de vulnerabilidades, ingeniería social, malware, etc.).

Escaneo / Fuerza bruta: se trata de un intento de acceso o explotación de un sistema, por lo general, desde una IP de un sistema que se encuentra comprometido. Engloba los intentos de acceso mediante adivinación o cracking de contraseña de un sistema publicado a Internet, escaneo de puertos, intento de explotación de una vulnerabilidad de un sistema publicado a Internet, etc.

Denegación de servicios (DoS/DDoS): se trata de ataques que dejan indisponible algún recurso, ya sea debido a un agotamiento de recursos o una inundación de tráfico o peticiones.

Esta lista se va ampliando indudablemente conforme al transcurso del tiempo ya que los ciberdelincuentes encuentras nuevas herramientas que pueden utilizar para vulnerar la seguridad de terceros.

Aunque nuestra experiencia con el ciberdelito aún es muy reciente, es evidente que el modelo actual de aplicación de la ley penal no es será de gran utilidad para hacer frente a estos en un futuro cercado, esto teniendo en cuenta que las características del ciberdelito difieren esencialmente de la delincuencia del "mundo real".

Tal vez la diferencia más amplia entre los dos es que a diferencia del delito del mundo real, el ciberdelito no requiere ningún grado de proximidad física entre la víctima y el victimario en el momento en que se comete el delito. El delito cibernético es un delito ilimitado, un delito sin fronteras. Puede ser cometido por alguien que se encuentra en cualquier parte del mundo contra una víctima que se encuentra en otra ciudad, otro estado, otro país. Todo lo que el perpetrador requiere es acceso a una computadora que esté conectada a Internet; con esto, puede infligir "daño" a alguien directamente, atacando su computadora, digamos, indirectamente, obteniendo información que le permita asumir su identidad y usarla para cometer fraude a gran escala.

El ciberdelito difiere del delito del mundo real también en otro aspecto importante, no siempre es un delito uno a uno porque no es un delito corporal, no es un delito terrestre; en efecto gran parte del delito cibernético ya es automatizado y se utilizan sistemas que realizan los procesos para la perpetración del delito sin necesidad de la intervención humana gracias a diversas herramientas tecnológicas, esta es una tendencia que apunta a acelerarse con los años. La automatización otorga al individuo la capacidad de utilizar la tecnología para multiplicar el número de delitos discretos que puede cometer en un período de tiempo determinado; un solo perpetrador puede cometer miles de delitos cibernéticos al mismo tiempo.

Otra complicación es que o sustancialmente todas las conductas involucradas en la comisión de un delito cibernético ocurren en un entorno electrónico; dado que un perpetrador no está físicamente presente cuando se comete el crimen, ya no se puede suponer que dejará rastros de evidencia en la escena del crimen. El ciberespacio hace que elespacio físico sea irrelevante. Se vuelve tan fácil victimizar a alguien que está al otro lado del mundo como a su vecino de al lado.

Además, el ciberespacio permite que los perpetradores oculten sus identidades; los ciberdelincuentes pueden disfrutar del anonimato en una escala que no es posible en el mundo real. En el mundo real, un delincuente puede usar una máscara y tal vez hacer otros esfuerzos para ocultar su identidad, pero ciertas características, como la altura, el peso, el acento, la edad, seguirán siendo evidentes. En el ciberespacio se puede lograr el perfecto anonimato, en consecuencia, es posible que los agentes no tengan forma de identificar a la persona que victimizó a alguien.

El ciclo vicioso del ciberdelito

Un aspecto que ha cambiado es la forma en que las víctimas comerciales denuncian su victimización. El auge de la ciberdelincuencia ha agravado una tendencia que existía antes, al menos en ciertas áreas del sector privado. La encuesta anual sobre delitos cibernéticos que lleva a cabo el Instituto de Seguridad Informática en conjunto con la Oficina Federal de Investigaciones ha demostrado consistentemente, por ejemplo, que solo un porcentaje muy pequeño de los ataques cibernéticos a las empresas se informa a las autoridades. Esto ocurre principalmente por 2 razones, la primera es el desconocimientoque tienen los directivos sobre la importancia de denunciar estos hechos y la otra es por temor a los efectos que tendrá la publicidad que acompaña a la investigación y un enjuiciamiento en sus operaciones comerciales.

La reticencia del sector privado a denunciar los delitos cibernéticos genera preocupación en las autoridades encargadas de hacer cumplir la ley por varias razones. Una es que, si las empresas no denuncian los delitos cibernéticos, el perpetrador de un delito puede volver a victimizar a esa empresa y/o usar las mismas tácticas para victimizar a otras empresas.

Marco jurídico actual del Ciberdelito

La eficacia de la justicia es trascendental para una estrategia efectiva que alcance una seguridad dentro del ciberespacio y la lucha contra el ciberdelito, esta debe incluir investigar, controlar y juzgar los delitos contra y a través de datos y sistemas informáticos, y obtener evidencia electrónica relevante a los efectos del proceso penal. Además, debe ser

lo adecuadamente ecuánime como para enfrentar a la evolución escalante de la tecnología y técnicas de ciberdelito que no quede obsoleta en el corto plazo ante el paso de los años.

La legislación contra el ciberdelito debe permitir un trabajo armonioso de cooperación internacional ya que la esencia de eludir las fronteras que posee el ciberdelito resulta en que la justicia penal no puede ser lo suficientemente eficaz sin una cooperación internacional, es por ello que los gobiernos del mundo han participado de convenios que buscan la armonización de estrategias colectivas de combate contra el ciberdelito, especialmente podemos mencionar el convenio de Budapest.

La convención sobre el Delito Cibernético, también conocida como la Convención de Budapest sobre el Delito Cibernético o la Convención de Budapest, como se menciona en su propio cuerpo normativo, es el primer tratado internacional que busca abordar los delitos informáticos y de Internet (delito cibernético) mediante la armonización de las leyes nacionales, la mejora de las estrategias de investigación y control y el acrecentamiento de la cooperación entre los países cooperantes.

El convenio de Budapest Incluye una diversidad de facultades de derecho procesal, tales como procesos para buscar, capturar, producir datos o interceptar comunicaciones, y la facultad de ordenar que los datos se guarden rápidamente. Es importante destacar que estos se refieren a pruebas electrónicas relacionadas con cualquier tipo de delito. Las delimitaciones deben hacerse bajo el estado de derecho y las salvaguardias. El tratado busca garantizar una cooperación internacional efectiva en temas de ciberdelincuencia y evidencia electrónica, combinando la asistencia legal mutua con medios rápidos de preservación de servidores ubicados en otros países. Asimismo, el ámbito de la cooperación no se limita al ciberdelito, sino que también incluye la cooperación sobre pruebas electrónicas encontradas en sistemas informáticos relacionados con cualquier delito.

Por lo tanto, el Convenio de Budapest sirve como una lista de verificación para estructurar un marco jurídico nacional de leyes procesales y sustantivas relacionadas con el ciberdelito y las pruebas electrónicas. Se puede decir que la Convención en su totalidad es un documento equilibrado, sensato y coherente que se considera mejor como un todo. Para los más de 70 países que son parte de la convención, el tratado es el marco legal para la cooperación internacional. El Convenio de Budapest está abierto a cualquier país que pretenda implementar sus reglas. De hecho, varios países de Latinoamérica y el Caribe han decidido seguir este camino como Argentina, Chile, Colombia, Costa Rica, Panamá, Perú y ratificado en nuestro país en el 2018.

Algunos países de Latinoamérica estructuraron disposiciones legales inspirándose en mayor parte sobre este convenio internacional. Entre ellos podemos encontrar a:

Argentina

Este país ha elaborado un completo marco jurídico para las herramientas digitales y las tecnologías de la información incluyendo la ley 26.388 de delitos informáticos modificando el código penal y la ley 25.326 de protección de datos, además se encuentra trabajando con el sector privado para incentivar los reportes de violaciones de la seguridad en el ciberespacio ante el índice de crecimiento de riesgos de seguridad cibernética principalmente a empresas.

Ante la expansión del gobierno digital y la comercialización electrónica en este país las autoridades se encuentran desarrollando estrategias de concientización para educar a los ciudadanos sobre la seguridad en el ciberespacio, entre estas campañas podemos citar al "Internet Sano" que tiene como objeto difundir prácticas sanas para el uso seguro de la red y "Con vos en la Web" que instruye a niños, encargados y profesores sobre el riesgo del grooming y en distintos institutos superiores se encuentran creando programas de capacitación en ciberseguridad e informática forense.

Brasil

La estrategia de Brasil para enfrentar el crimen cibernético se basa en las leyes n° 12.965/2014 del marco de Derechos Civiles para Internet y la Ley n° 12.737 que tipifica el ciberdelito formalmente. La oficina de Represión de la Delincuencia Cibernéticadependiente de la Policía Federal es la principal autoridad encargada de investigar los ciberdelitos.

Perú

El marco legal que ampara la estrategia peruana contra la ciberdelincuencia se basa en las leyes 27309 que incorpora los delitos informáticos al Código Penal, la 29733 de protección de datos y la ley 30096 que establece las normas jurídicas afines a la ciberdelincuencia. La División de Investigación de Delitos de Alta Tecnología de la Policía Nacional del Perú máxima autoridad para el control de la ciberdelincuencia.

Uruguay

Sobre el marco jurídico respecto a la ciberdelincuencia en Uruguay podemos mencionar que encontramos la ley n° 18.331 de Protección de datos, pero es inexistente aún una legislación penal destinada a los ciberdelitos. La unidad de ciberdelitos de la Policía Nacional es el órgano responsable de la investigación de los delitos cibernéticos.

Chile

Chile es el país de la región que más actualizado se encuentra a la fecha en lo que a la lucha contra el ciberdelito respecta ya que este año promulgó la nueva ley 19.223 sobre Delitos Informáticos que se elaboró siguiendo los parámetros establecidos en el convenio de Budapest, esta ley moderniza algunos conceptos como el de sabotaje informático, e incorpora nuevos ciberdelitos como la falsificación y el fraude informático. Dota de mayores herramientas y mejores herramientas relacionadas con el ciberdelito especialmente en el derecho procesal en temas relacionados a la cadena de custodia de pruebas electrónicas.

Marco jurídico Nacional

En nuestro país la unidad especializada para enfrentar los hechos los hechos punibles realizados en el ciberespacio es la Unidad Especializada de Delitos Informáticos que tiene competencia exclusiva en los siguientes delitos informáticos: Intercepción,

preparación al acceso indebido de datos, acceso indebido a datos, alteración de datos, sabotaje a sistemas informáticos, alteración de datos relevantes, estafa mediante sistemas informáticos, falsificación de tarjetas de crédito y débito y acceso indebido a sistemas informáticos, esto conforme a las Resoluciones Nº 3459/10 y 4408/11.

En Paraguay se agregaron al Código Penal la mayoría de las disposiciones sugeridas e implementadas por el convenio de Budapest mediante la ley 4439 del 2011 incluyendo los ciberdelitos, así como la pornografía infantil. Al respecto de las denuncias de los ciberdelitos de los cuales son víctimas las instituciones del sector privado, estos tienen la obligación de informar los hechos punibles a las autoridades correspondientes conforme ala ley 1286/98.

Antes de ir concluyendo este artículo es válido dar un destaque especial al CERT o Centro de Respuestas a Incidentes Cibernéticos de nuestro país que es un órgano encargado de encabezar la respuesta a incidentes cibernéticos que vulneran el ciberespacio dentro de nuestro territorio nacional.

El CERT-PY brinda un servicio permanente de gestión de incidentes cibernéticos, disponible para cualquier persona u organización, sin ningún costo. Cualquier ciudadano, empresa, institución pública u organización extranjera puede reportar un incidente cibernético que afecte a un sistema de información del ecosistema digital nacional, propio o de terceros, según se menciona en el mismo informe de seguridad del 2020, publicado por el CERT.

Generalmente cada país tiene su equipo de respuesta ante incidentes informáticos, en algunos tienen como nombre CSIRT y en otros CERT, estos trabajan la mayor parte del tiempo en conjunto para poder dar una respuesta eficiente a los incidentes informáticos ya que como hemos visto hay altas chances de que estos se realicen de forma transnacional por lo que la cooperación internacional es clave.

En nuestro país el CERT tiene a su cargo el análisis previo del incidente cibernético, la aplicación de acciones de contención inmediatas, la investigación y la propuesta de recomendaciones pertinentes para la corrección y prevención futura.

Conclusión

Los ciberdelitos presentan muchos desafíos para la ley, tanto civil como penal. Uno de los desafíos más críticos que enfrenta la ley es garantizar la aplicación de la ley penal en el ciberespacio y poder establecer una protección eficaz para todos los internautas tanto individuos como entidades privadas y públicas. Como se explicó a lo largo de este artículo, el delito cibernético se diferencia en varios aspectos fundamentales del delito del mundo real, el tipo de delito para el cual se desarrolló nuestro modelo existente de aplicación de la ley. Como resultado, el modelo tradicional actual que de a poco se va reformando no es un medio eficaz para hacer frente a la ciberdelincuencia.

Hay buenas razones para creer que estamos presenciando el surgimiento de un nuevo modelo de aplicación de la ley, al menos con respecto al delito cibernético. Si bien es demasiado pronto para especular con alguna especificidad sobre la forma final que tomará este modelo, es posible notar varias características que seguramente persistirán. Debido a que es el producto de un proceso evolutivo que está cambiando nuestro orden social básico, del estado-mercado, el nuevo modelo necesariamente quitará énfasis al hecho de que el estado garantiza ciertos derechos y protecciones a sus ciudadanos. Enfatizará las oportunidades y obligaciones de los ciudadanos. Para el delito cibernético, esto significaque veremos la evolución de un sistema en el que los ciudadanos y los funcionarios encargados de hacer cumplir la ley trabajen juntos para garantizar nuestra seguridad colectiva frente al delito, en particular el delito cibernético.

Bibliografía

CERT-PY. (2020, marzo). Estado de la ciberseguridad en Paraguay (N.º 3). Ministerio de Tecnologías de la Información y Comunicación.

Computer security institute. (2012, abril). Cybercrime bleeds united states corporations, survey shows; financial losses from attacks climb for third year in a row (N.º 1). *Rutgers Computer And Technology Law Journal*.

Convenio sobre cibercrimen, Budapest, 23 de noviembre de 2001.

Jordán, T. (1999). Cyberpower: The Culture and Politics of Cyberspace and the Internet (El ciberespacio: la cultura y la política del ciberespacio). Routledge.

Ley Nº 1286. (1998). Código Procesal Penal. Asunción, Paraguay.

Ley Nº 4439. (2011). Modifica y amplia varios artículos de la Ley n° 1160/97 código penal. Asunción, Paraguay.

Resoluciones Nº 3459/10 y 4408/11 de la FGE.

Simón Kemp. (2022, Enero). *Digital 2022: global overview report.* DATA REPORTAL https://www.datareportal.com/

Tellez, J. (1999). Derecho Informático (1.a ed.). Mcgraw Hill Edducation.