Revista Iberoamericana de Derecho, Cultura y Ambiente

Edición Nº 5 – Julio 2024

www.aidca.org/revista

CIBERCRIMEN Y DELITOS INFORMATICOS

Por María Inés Amato[1]

INTRODUCCION

A finales de los años 70, del siglo XX, nacen los delitos informáticos y los cibercrímenes: que comprenden los daños informáticos, transferencias no consentidas de activos, obstaculización de datos e infraestructura informáticos, etc., que demostraron la existencia de una serie de factores dogmáticos y político-criminales que obligan a repensar e incluso replantear muchas de las nociones y categorías dogmáticas tradicionales.

Son delitos que lesionan o ponen en peligro efectivo la confiabilidad(confidencialidad), la integridad y la disponibilidad de los datos, los sistemas y las infraestructuras informáticas necesarias para el adecuado funcionamiento social.

Se trata de conductas punibles art.9 Código Penal, que tienen lugar en el ciberespacio, que existe como una realidad simulada y que, si bien favorece la

[1] Abogada (Universidad de Morón). Licenciada en Psicología (UBA). Doctora en Psicología Clínica (U. J.F. Kennedy). Especialista en Violencia Familiar (UBA). Perito forense en juzgados civiles. Abogada del Niño (Colegio de Abogados de La Matanza). Master Internacional en Mediación, Resolución de Conflictos y Justicia Restaurativa (Formación Ejecutiva). Panelista en Radio Judicial El Mundo. Escritora.

gestión social globalizada en aspectos políticos, sociales y económicos, también fortalece nuevos riesgos delictivos que se reproducen en una sociedad hiperconectada, mediática y altamente vulnerable por su analfabetismo digital.

DESARROLLO

El cibercrimen como modalidad criminal sitúa a la doctrina contemporánea frente a las transformaciones sustantivas del delito y de la pena. En 1er lugar se advierte la existencia de una definición del delito más compleja y especializada que la noción de los delitos realizados en el mundo físico porque no solo abarca nuevas realidades como el ciberespacio , o por la exigencia del empleo de nuevas técnicas especializadas(como medio) y de objetos de protección prevalentemente inmateriales, sino también porque los comportamientos involucran una compleja transformación de los elementos típicos objetivos y subjetivos sobre todo de la acción y de sus resultados.

En 2do lugar, porque la sociedad moderna, deconstruida y reconstruida como una sociedad digitalmente modificada, tiene como base de funcionamiento la gestión de la información, los datos y las infraestructuras informáticas necesarias para las subsistencia e interacción de sus miembros.

En 3er lugar, porque los avances tecnológicos hacen cada vez más compleja la delimitación de las categorías dogmáticas de la conducta punible, como estructuras jurídicas que permiten explicar mejor estas nuevas formas de criminalidad.

Diferencia entre delito informático y ciberdelito.

El 1° se vale de elementos informáticos para su perpetración, mientras que el 2°se refiere a una posterior generación delictiva vinculada a las tecnologías de la información y comunicaciones.

En este sentido la criminalidad informática consiste en la realización de un nuevo tipo de actividades que reúnen los requisitos que delimitan el concepto de delito, y son llevados a través de un elemento informático.

El Convenio de Budapest sobre Ciberdelincuencia es un tratado internacional creado en el año 2001 impulsado por el Consejo de Europa[2], con el objetivo de incrementar la cooperación internacional y generar marcos legales y armónicos entre las naciones para hacer frente a los delitos informáticos y a la actividad criminal en internet.

El objetivo principal de este instrumento, definido en el preámbulo es establecer una política común y alineada entre países, orientada a la protección de la sociedad contra la ciberdelincuencia. Esto se alcanza tipificando los delitos informáticos de forma similar en todas las naciones, unificando normas procesales y a través de una cooperación internacional armónica. Pretende ser una guía para que los países desarrollen políticas nacionales integrales y alineadas contra el cibercrimen.

En el Convenio de Budapest sobre la ciberdelincuencia (2013) se agruparon los delitos informáticos en los siguientes grupos:

1- Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos (acceso e interpretación ilícita, así como la interferencia de datos).

2. Delitos por su contenido, tales como la pornografía infantil y xenofobia.

3. Delitos relacionados con la informática, como la falsificación y fraude.

4. Delitos relacionados con las infracciones a los derechos de propiedad.

Los países que firmaron el Convenio fueron, Argentina, Bolivia, Costa Rica, Guatemala, México, Paraguay y Perú, se comprometieron a modificar la legislación penal, seguido a esto, los países de Brasil, Chile, Colombia y Venezuela introdujeron leyes específicas.

Chile, si bien no define ni ciberdelitos ni delitos informáticos, en el Decreto N° 83, de 2017, de Relaciones Exteriores que promulga el Convenio de Budapest, entre las Declaraciones sobre Ciberdelincuencia, el Decreto dispone:

[2] Convenio de Budapest sobre la Ciberdelincuencia en América Latina. Derechos Humanos y Tecnología en América Latina

a) La República de Chile declara que exigirá una intención delictiva determinada en el sujeto activo, para penar las acciones descritas en los artículos 2 y 3 del Convenio sobre Ciberdelincuencia, conforme lo requiere el art.2 de la Ley 19.223 sobre delitos informáticos.

b) La República de Chile, declara que exigirá el ánimo fraudulento que produzca un perjuicio a 3ros para penar las acciones descritas en el art.7 del Convenio sobre la Ciberdelincuencia, conforme lo requiere el art.197 del Código Penal.

El art.2 del Convenio se refiere al "acceso ilícito", obligando a la tipificación como delito el acceso deliberado e ilegitimo a todo o parte de un sistema informático, pudiendo exigir los Estados, que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos u otra intención delictiva, o en relación con un sistema informático conectado a otro sistema informático.

El art.3, del citado convenio, se refiere a la" interceptación ilícita", obligando a los Estados partes, a tipificar como delito, la interceptación deliberada e ilegítima por medios técnicos de datos informáticos en transmisiones no publicas dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos, pudiendo exigir los estados, que el delito se cometa con intención delictiva o en relación con un sistema informático conectado otro sistema informático.

Por su parte el art.2 de la Ley 19.223, sobre delitos informáticos, recogiendo ambos conceptos (acceso e interceptación) para su penalización dispone que:

"El que con ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepta, interfiera o accede a él, será castigado con presidio menor en su grado mínimo a medio".

Por otra parte, el art.7 del Convenio, remite al decreto promulgatorio que obliga a los Estados a tipificar el " delito de falsificación informática", que consiste en la

introducción, alteración, borrado o supresión deliberados e ilegítimos de datos informáticos que genere datos no auténticos con la intención de que sen tomados o utilizados a efectos legales como auténticos, con independencia de que los datos sean legítimos e inteligibles, pudiendo los Estados, que exista una intención dolosa o delictiva similar para que se considere que exista responsabilidad penal.

En síntesis, Chile se compromete a tipificar a la ciberdelincuencia y a los delitos informáticos, exigiendo una intención delictiva determinada en el sujeto activo/artículos 2 y 3 del Convenio) y animo fraudulento que produzca un perjuicio a 3ros (art. 7 del Convenio).

Estados Unidos, en cuanto al concepto de “delito cibernético”, fue el 1ro en acuñar el concepto de cibercrimen, utilizando una acepción amplia del mismo, que comprende aquellas situaciones en que el elemento informático se encuentra en el objeto de la conducta penada, por ej. Intromisión ilegal a bancos de datos, y aquellas en que dicho elemento es el medio para realizar un fin ilícito por ej. Una estafa por internet.

La legislación norteamericana tipifica bajo la denominación genérico de ciberdelitos, figuras como el terrorismo (Ley USA Patriot), obscenidades, diversas figuras de pornografía, prohibición de dominios engañosos, prohibición de uso de recursos públicos para adquisición de ordenadores sin filtros, reducción de menores para propósitos sexuales, protección de copyright: difamación, amenazas y acoso cibernético, etc., todos ellos cometidos por medios informáticos.

Se considera ciberataques puros, a un conjunto de conductas ilícitas, de infracciones que pueden considerarse totalmente nuevas al estar caracterizadas por dirigirse contra los nuevos servicios y solo es posible producir la ilicitud de estas infracciones en el ciberespacio.

Entre estas infracciones encontramos: a) El hacking, que consiste en la forma de destrucción, modificación o acceso a datos de empresas o de particulares. Según estudios realizado en Estados Unidos, casi el 50%de este tipo de ataques se realiza por medio de una acción desleal, generalmente de un insider que

aprovecha su posición en la empresa para dañarla o vender su información a otros.

En sentido estricto se trata de una conducta que conlleva a la violación de una esfera de exclusividad reservada al titular del sistema, haya o no en él información privada o confidencial.

El hacking, es siempre un acceso remoto, esto es, realizado a distancia por el sujeto, que normalmente a través de Internet, se entromete en un sistema sin tener contacto físico con él.

Todo hacking implica la intromisión no autorizada y por ello es un acto de negación de la esfera de decisión de sujetos privados cuya seguridad es esencial para que internet se convierta en un medio de comunicación y de transmisión universal.

b) Infecciones de malware y otras formas de sabotaje cibernético.; consiste en el envió de redes telemáticas de virus informáticos que aprovechan la inmensidad de la red para multiplicarse y acceder a miles de terminales, como cualesquiera otras formas de destrucción de archivos o datos terminales concretos y determinados, con fines industrial o e daño individual.

Representa un autentica amenaza en la actualidad, ya que, al fin y al cabo, es el hecho de que los sistemas informáticos están conectados entre si en un ciberespacio trasnacional y universalizado, lo que acrecienta los riesgos de que se produzcan daños al sistema o a los datos contenidos en él.

El sabotaje cibernético puede afectar bien a los propios sistemas informáticos y demás elementos de hardware que lo conforman y que son evaluables económicamente; bien a la información contenida en los citados sistemas y que puede tener un valor económico o personal, en el sentido sentimental y relacionado con su propia dignidad, para el sujeto pasivo; o bien a la propia funcionabilidad del sistema informático en el marco de la actividad económica de que se trate.

Hoy en día, ya no solo es posible la destrucción de la información, sino también la paralización de la difusión de la misma, lo cual obviamente supone la neutralización de los servicios relacionados.

c) Malware. Es la más popular de las formas de sabotaje cibernético, se lleva a cabo mediante la infección de virus destructivos, destinados a dañar, controlar o modificar el sistema informático.

No solo aumentan los virus, sino que al igual que el ente biológico, también cambian adaptándose a las nuevas necesidades.

Los riesgos de la información devienen en gran parte de la amenaza de tal forma de malware destructivo; son millones de personas e instituciones que han perdido informaciones valiosas (personal o económicamente) a causa de un archivo enviado remotamente y en muchos casos de forma aleatoria y expansiva. De este modo, los primeros infectados y afectados reenvían involuntariamente a otros por medio del correo electrónico el malware malicioso, creándose una cadena destructiva que puede causar pérdidas millonarias.

El envió de malware, en la actualidad no es más que un comportamiento inicial necesario para la realización del ataque final consistente en una agresión dirigida al patrimonio o bien a la intimidad de los usuarios.

d) Los ciberfraudes.En. En este grupo, entrarían los fraudes de internet, en los que las redes telemáticas se convierten en un instrumento para lograr un beneficio patrimonial derivado de un perjuicio patrimonial a una víctima.

Son muchas las formas en las que se puede lograr acceder al patrimonio de terceros, utilizando las múltiples formas de relación comercial existente en el ciberespacio, así como las propias debilidades de seguridad de los sistemas informáticos que dan acceso al patrimonio, o indirectamente a él, al contener las claves o datos bancarios de los usuarios. Algunos de los más conocidos son: los distintos fraudes de tarjeta de crédito, los fraudes de cheques, las estafas de inversión, las conocidas estafas de la lotería, las ventas online defraudatorias en las que no se envía el producto comprado (o se envía con otras características), entre otros.

e) El robo de identidad o phishing. Es un delito grave, tiene lugar cuando una persona utiliza la información de identificación personal como, nombre, número de seguro social o la tarjeta de crédito de otra persona sin permiso para cometer fraude u otros delitos.

¿Como se castiga? El art. 401 del Código Penal castiga este delito con pena de prisión de 6 meses a 3 años. La acción descrita en el tipo penal es la de usurpar el estado civil de otro.

Que podemos hacer, en un caso como este, la clave es desconfiar, si alguna de las siguientes situaciones se presenta en un mail: a) Solicitud de datos personales o información de la cuenta o contraseña.; b) Si informan cambios o problemas de seguridad de algunas de las cuentas del usuario; c) El mensaje requiere una acción urgente o inmediata del usuario; d) El mensaje no está dirigido explícitamente , no está personalizado; e) El tono de la comunicación no está a la altura del emisor aparente, ni presenta la calidad necesaria para la ocasión, por ej. El mensaje contiene faltas de ortografía, errores gramaticales o incoherencias f) El mensaje no proviene de un contacto conocido o no lleva firma del remitente.

Si crees que los datos han sido comprometidos, se debe cambiar inmediatamente las contraseñas de acceso y comunicarse con el soporte técnico correspondiente de la cuenta o sistema afectado.

Se debe denunciar, pedir asistencia al CONICET.

Guardar cualquier evidencia de estafa y perjuicio. Una vez realizada la denuncia, proceder de la forma que indique la autoridad interviniente.

f) Delitos informáticos contra la integridad sexual. El Código Penal sanciona las siguientes conductas en el art.128” producir, financiar, ofrecer, publicar, facilitar, divulgar o distribuir cualquier representación de una persona menor de 18 años dedicada a actividades sexuales explicitas o de sus genitales”

“Tener representaciones de personas menores de edad de actividades sexuales explicitas o de sus partes genitales para distribuirlas o comercializarlas”.

También sanciona el ciberacoso a personas menores de edad(grooming). Este delito consiste en tomar contacto con una persona menor de edad a través de medios de comunicación electrónica (redes, mail, chat, etc.) para comer alguno de los delitos contra la integridad sexual.

La ley 26.904, define al grooming o ciberacoso como" la acción en la que una persona por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contacte a una persona menor de edad con el propósito de cometer cualquier delito contra la integridad sexual de la misma"

Fases del Online Grooming.

1. La creación de un vínculo de confianza: El agresor contacta con el niño/a y establece un vínculo de confianza. Le hace regalos, empatiza a un nivel profundo, escucha sus problemas y aprovecha esa información que el niño brinda para chantajearlo después.

2. El aislamiento de la víctima. En esta fase el agresor persigue arrancar la red de apoyo natural del menor (familiares, amistades, docentes, etc.) dejándolo desprotegido. De esta manera insiste en la necesidad de mantener todo en secreto.

3. La valoración de los riesgos. El agresor tiende a asegurarse su posición, así suele preguntar a la víctima si alguien más conoce su relación e intenta averiguar quien tiene acceso al ordenador o dispositivo que utiliza el menor.

4. Conversaciones sobre sexo. Una vez que la Niña/o se siente en confianza, el abusador empieza introducir conversaciones sexuales de manera paulatina. Busca que la víctima se familiarice con la temática sexual.

5. Las peticiones de naturaleza sexual: En esta última fase el abusador utiliza la manipulación, las amenazas, el chantaje o la coerción par que la víctima le envié material sexual, relate fantasías sexuales o la relación culmine con un encuentro físico.

La ley Mica Ortega. Esta ley lleva el nombre de Micaela Ortega, que fue asesinada en 2016 por un hombre que la contacto por Facebook, haciéndose pasar por un menor de edad. El objetivo de esta ley es prevenir, sensibilizar y generar conciencia en la población sobre la problemática del grooming o ciberacoso a través del uso responsable de las tecnologías de la información y la comunicación (Tics)y de la capacitación de la comunidad educativa en su conjunto.

Se recomienda no borrar ningún contenido del teléfono o la computadora que el menor o la menor haya recibido, ya que las conversaciones, las imágenes y los videos que se hayan intercambiado con el supuesto acosador, deben ser guardados como prueba

Se debe realizar la denuncia policial para iniciar la investigación el caso, puede hacerse presencialmente en una comisaría o fiscalía, también de manera online en el Ministerio Publico Fiscal de la Ciudad Autónoma de Buenos Aires.

CONCLUSIONES

La ley 26.388, denominada de delitos informáticos, cubrió un importante vacío legal que hasta ese momento existía.

En los inicios de internet, no se buscaba su regulación legal, ya que se trataba de una red mundial de consultas y comunicación., su esencia era la libertad de acción.

Con el paso del tiempo y con los ataques terroristas que utilizaban la red para esa comunicación, esa primera idea quedo sin efecto por lo tanto los estados comenzaron a controlar todo aquello que circulaba por la red.

Así es, con el aumento de los delitos cometidos por medios electrónicos y la falta de legislación, llevo a los países a elaborar un Convenio Internacional con el fin de regularlo. Es así, que, en la Ciudad de Budapest, en noviembre de 2001, se firmó un Convenio sobre Cibercriminalidad, en el cual los países intervinientes se comprometieron a contar con un mayor control en la utilización y seguridad de Internet.

Internet va en aumento y en crecimiento, día a día nos encontramos con nuevas opciones y posibilidades para realizar a través de la web.

Las niñas/os y adolescentes han nacido en la era de la tecnología, por lo tanto, deben saber que las redes sociales pueden ser de mucha ayuda a la hora de buscar información y contactos, pero también puede ser una fuente inagotable para la delincuencia si no saben darle un uso correcto. En las redes sociales generalmente comparten nombre, apellido, domicilio, colegio, gustos, foto de la familia, de la novia/o, de las vacaciones, del club, comparten información con cualquier persona conocida y desconocida, permiten ingresar y aceptar como amigos a amigos de sus amigos y así sucesivamente, hasta el punto de aceptar cualquier desconocido, no tienen conciencia al cual están sometidos. Es la obligación de los adultos educar, enseñar y prevenir.

Debemos prevenir desde los hogares, educando a niñas, niños y adolescentes en el verdadero uso de las herramientas informáticas para evitar que caigan en manos de delincuentes cibernéticos.

BIBLIOGRAFIA

ALMENAR Schurjin, Daniel. Delitos Informáticos en Argentina. Revista Pensamiento Penal,2022

Convenio de Budapest sobre la Ciberdelincuencia en América Latina. Derechos Humanos y Tecnología en América Latina

HERRERA Gonzales H. Problemática del bien jurídico de los nuevos delitos y telemáticos. SAIJ. Sistema Argentino de Información Jurídica, 2006

LUCERO, Pablo y Alejandro Kohen. Delitos informáticos. Ediciones DyD

LUX Mayer, Laura. El bien jurídico protegido en los delitos informáticos. Revista Chilena de derecho.Vol.44, n°1.Santiago, abril 2017

RIQUET, Marcelo Alfredo. Delitos informáticos.www.delitosinformaticos.com

SORBO, Hugo Daniel. Delitos Informáticos. Aspectos a tener en cuenta de la ley 26.388. UTSUPRA,2013

Telefónica Tech.En que consiste el Convenio de Budapest y como regula la Ciberdelincuencia. Enero 2020

UR