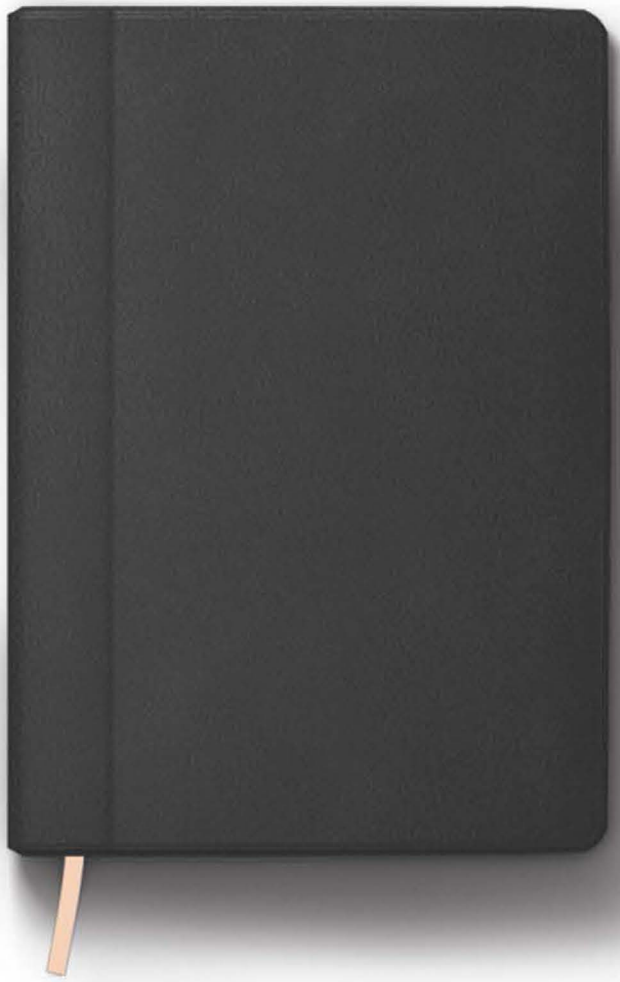
CUADERNOS DE POSGRADO 2024

SECRETARÍA DE POSGRADO



FACULTAD DE DERECHO
Y CIENCIAS SOCIALES Y POLÍTICAS
UNIVERSIDAD NACIONAL DEL NORDESTE

UNIVERSIDAD
NACIONAL
DEL NORDESTE

Cuadernos de Posgrados

| 2024 |

Cuadernos de posgrados 2024 / Carla Camila Jarko ... [et al.] ; Compilación de Mónica Andrea Anís ; Director Nahuel Pellerano ; Hilda Zulema Zárate. - 1a ed adaptada. - Corrientes : Universidad Nacional del Nordeste. Facultad de Derecho y Ciencias Sociales y Políticas, 2025.
Libro digital, PDF

Archivo Digital: descarga y online
ISBN 978-631-6623-11-9

1. Derecho. I. Jarko, Carla Camila II. Anís, Mónica Andrea, comp. III. Pellerano, Nahuel, dir. IV. Zárate, Hilda Zulema, dir.
CDD 346.02

Cibercrimen y Delitos Informáticos

| Claudio Cesar Dalmao |

»

Introducción

Los ciberdelitos engloban una amplia gama de actividades ilícitas que se llevan a cabo utilizando medios electrónicos o digitales. Desde el hackeo de cuentas hasta la difusión de contenido ilegal, pasando por estafas en línea y el robo de identidad, la variedad de delitos cibernéticos es extensa y en constante crecimiento.

En Argentina, al igual que en el resto del mundo, los ciberdelitos son una problemática que va en aumento. La creciente digitalización de la sociedad y el uso masivo de internet han convertido a nuestro país en un blanco atractivo para los ciberdelincuentes.

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 criminales que obligan a repensar e incluso replantear muchas de las nociones y categorías típicas 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, que tienen lugar en el ciberespacio, que existe como una realidad simulada y que, si bien favorece la ges-

tión 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 moderna frente a las transformaciones sustantivas del delito y de la pena. En primer 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 segundo lugar, porque la sociedad moderna, devenida a 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 tercer lugar, porque los avances tecnológicos hacen cada vez más compleja la delimitación de las categorías 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 realiza-

ción 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, 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, 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, entre ellos Argentina,, se comprometieron a modificar la legislación penal, seguido a

esto, los países de Brasil, Chile, Colombia y Venezuela introdujeron leyes específicas.

Estados Unidos, en cuanto al concepto de "delito cibernético", fue el primero 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. 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.

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.

Conclusiones

"La mejor estrategia es sin dudas LA EDUCACIÓN y LA PREVENCIÓN" La Realidad Argentina. La Ley 26.388

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.

¿Qué es la Ley 26.388?

Esta ley, sancionada en 2008, introdujo una serie de modificaciones al Código Penal Argentino, incorporando figuras delictivas específicas para combatir los delitos informáticos. Su principal objetivo fue actualizar el sistema penal para hacer frente a la creciente incidencia de los ciberdelitos y brindar herramientas legales para perseguir a los responsables.

Impacto de la Ley 26.388

La Ley 26.388 ha tenido un impacto significativo en la legislación argentina, ya que:

- *Tipificó nuevos delitos:* Introdujo nuevos tipos penales como el acceso ilegítimo a sistemas informáticos, la interceptación de datos, la falsificación informática y la estafa informática, entre otros.
- *Actualizó figuras delictivas preexistentes:* Adaptó figuras delictivas tradicionales, como el robo y la estafa, a la realidad digital.

- *Estableció penas:* Definió las penas correspondientes a cada delito informático, permitiendo así una mayor eficacia en la persecución y sanción de estos actos ilícitos.
- *Brindó herramientas a los jueces:* Proporcionó a los jueces las herramientas necesarias para interpretar y aplicar la ley en casos concretos.
- *Fomentó la investigación:* Impulsó la investigación y persecución de los ciberdelitos, al establecer mecanismos de cooperación entre las fuerzas de seguridad y los organismos judiciales.

¿Cuáles son algunos de los desafíos que aún persisten?

A pesar de los avances introducidos por la Ley 26.388, aún existen desafíos a superar:

- *Evolución constante de la tecnología:* La rápida evolución de la tecnología hace que los ciberdelitos se adapten constantemente, lo que exige una actualización continua de la legislación.
- *Complejidad de las investigaciones*: La investigación de ciberdelitos suele ser compleja y requiere de conocimientos técnicos especializados, lo que puede dificultar la obtención de pruebas.
- *Jurisprudencia en desarrollo:* La jurisprudencia en materia de ciberdelitos aún se encuentra en desarrollo, lo que genera cierta incertidumbre en la aplicación de la ley.

En resumen, la Ley 26.388 representa un paso fundamental en la lucha contra los ciberdelitos en Argentina. Sin embargo, es necesario continuar trabajando para actualizarla y adaptarla a los nuevos desafíos que plantea el mundo digital.

Bibliografía

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

ABOSO, Gustavo E. (2022). Ciberdelitos