Tesina

Facultad de Derecho y Ciencias Sociales

LOS CIBERDELITOS Y LA REPERCUSIÓN DE LAS ESTAFAS INFORMÁTICAS DURANTE LA CUARENTENA

AUTOR: SOFIA BELEN IANNICELLI GODOY

MATRÍCULA: 101- 33777

TUTORA: ANIBAL J. MATHIS

CARRERA:ABOGACÍA FACULTAD DE DERECHO

AÑO 2021

INDICE GENERAL

Resumen

La aparición de la era tecnológica implica nuevos paradigmas para la sociedad, tanto positivos como negativos. Resulta indiscutible el hecho de que vivimos en una sociedad digital que influye en el desarrollo económico, social, de educación y la posibilidad de estar relacionados con cualquier parte del mundo.

Si bien los medios de comunicación y las tecnologías resultan prácticas para muchos aspectos de la vida, podemos encontrar la contracara. Este lado oscuro se puede ver reflejado en la delincuencia, criminalidad y con la aparición de nuevas modalidades de comisión de los delitos tradicionales.

Los ciberdelitos se cometen gracias a las ventajas y facilidades que ofrecen la digitalización de las comunidades. Les proporciona a los ciberdelincuentes numerosas herramientas para la comisión de las conductas ilícitas, asegurando muchas veces el anonimato y la impunidad debido a la falta de conocimiento, equipos, capacitación, poca legislación en la materia y falta de medidas de seguridad de los usuarios de internet para poder engañarlos, estafarlos, robarlos o extorsionarlos generando un ambiente propicio para quienes practican estas actividades.

En definitiva, la aparición de los delitos informáticos y la evolución de la criminalidad implica en el Derecho grandes transformaciones desde la ampliación de los bienes jurídicos objeto de protección, tipificación de las conductas, necesidad de dictar nuevas leyes, de capacitación al personal de la Justicia, entre otros.

Para una mejor comprensión de la problemática planteada se identificaran los delitos informáticos, sus características y la regulación vigente en nuestro país.

Para ello se plantearon los siguientes objetivos:

- Conceptualización de las conductas típicas, antijurídicas y culpables que se genera en virtud de la tecnología.
- Definir las características de quienes cometen esta clase de delitos y de sus víctimas.
- Establecer el modus operandi,
- Dificultad en la recolección de evidencia para encontrar al autor del delito.
- Determinar el tipo de herramientas que contamos para la efectiva investigación.

Palabras claves: Derecho Penal- Delitos informáticos- Código Penal- Impacto social- Actualidad

CAPÍTULO I: Primeras aproximaciones sobre los delitos informáticos.

En este primer capítulo se analizará a priori el fenómeno de los delitos informáticos estableciendo sus características generales y sujetos intervinientes, para a partir de allí relacionarlo con la normativa vigente en nuestro país.

1. El término de delitos informáticos

La Organización para la Cooperación Económica y el Desarrolla delimita a los delitos informáticos como *"Cualquier conducta, no ética, o no autorizada, que involucra el procesamiento automático de datos y/o la transmisión de datos*"[1].

El Convenio sobre Ciberdelito o también llamado el Convenio de Budapest creado en el año 2001 con la posterior adhesión de Argentina en diciembre del 2017 establece que son delitos informáticos "*los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas redes y datos".* [2]

Los instrumentos nacionales e internacionales no buscan definir el delito per se, sino que describen una lista de actos o conductas que podrían constituir un delito cibernético sin establecer un término legal técnico.

Entre la conceptualización doctrinaria podemos encontrar en su libro "Derecho informático" del Dr. Julio Téllevez Valdés como aquellos delitos que se pueden clasificar en sus formas típicas y atípicas, entendiendo por la primera *a "las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin"* y por las segundas a *"actitudes ilícitas en que se tienen a las computadoras como instrumento o fin"[3].*

Por otra parte, el Dr. Alexander Díaz García establece que esta clase de delitos deben ser observado desde tres puntos de vista, *"Como fin en sí mismo, pues el computador puede ser objeto de la ofensa, al manipular o dañar la información que este pudiera contener; Como medio: Como herramienta del delito, cuando el sujeto activo usa el ordenador para facilitar la comisión de un delito*

[1] OCDE: "Delitos de Informática: análisis de la normativa jurídica" Recuperado de: ocde.org
[2] Convención sobre cibercrimen, disponible (en inglés) en https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561. Existe una traducción no oficial al español disponible en https://rm.coe.int/16802fa41c
[3] Téllez Valdés, Julio: "Derecho informático" - 4ª ed. - Ed. Mc Graw Hill - México - 2004 - págs. 165-167

tradicional; Como objeto de prueba: Los computadores guardan pruebas incidentales de la comisión de ciertos actos delictivos a través de ellos"[4].

Entre los distintos organismos y autores han establecido diferentes apreciaciones para señalar las conductas delictivas de los delitos informáticos, electrónicos, crímenes por internet, delitos relacionas con las computadoras ya que no existe una definición propia de carácter universal.

Entre los distintos conceptos podemos ver que coinciden en que se trata de un delito donde la conducta humana merece ser penado y que el sujeto activo posee condiciones específicas para imputarle dicha conducta.

2. Aspectos generales y características

Es menester enfatizar que Internet es una red mundial que posee conexiones instantáneas, con una estructura descentralizada que permite que estas sean en tiempo real entre personas en cualquier parte del mundo. Esto implica una oportunidad para cometer delitos debido que las fronteras, la distancia y el tiempo no resultan relevantes como en los delitos tradicionales.

En consecuencia, estas características vinculadas abrieron un gran escenario de oportunidad criminal para la comisión de delitos lo que conlleva a una alta dificultad de investigación y persecución por parte de la Justicia.

El ciberespacio posee un alcance global lo que permite a los delincuentes que puedan actuar desde cualquier lugar en el mundo sin necesidad de trasladarse, buscar las víctimas más vulnerables, eliminar las barreras sociales que se podrían encontrar si la interacción fuese en persona y efectuar ataques evitando la persecución gracias a la deslocalización, lo que implica muchas veces la persecución del delito con ayuda de la Cooperación Internacional.

La utilización de diferentes herramientas para la navegación anónima le puede otorgar cierta discrepancia a los sujetos, detrás de un número de IP falso, correo electrónico o perfil y aunque pudiese seguirse el rastro digital, conocer desde que terminal y a través de que servidor se operó resulta demasiado difícil al momento de individualizar al sujeto activo que realmente lo perpetró.

Se caracterizan por ser trasnacionales o trasfronterizos, provocando un problema de competencia entre las distintas jurisdicciones de los Estados, la discrepancia existente en la legislación aplicable, si constituye o no un delito y en consecuencia si la conducta es pasible de una pena. Cabe destacar que a su vez, preexisten paraísos informáticos constituidos con un alto grado de impunidad para el delincuente.

[4] Diaz García, Alexander: "El bien jurídico tutelado de la información y los nuevos verbos rectores en los delitos informáticos" Recuperado de: oas.org

Son considerados instantáneos relacionados con las nuevas tecnologías, ya que el momento de realización es instantáneo más allá del tiempo que podría llevar la inteligencia preliminar o preparación. El delito se perfecciona al momento en que el delincuente realiza la acción.

Es posible que con estas conductas se vea afectado más de un bien jurídico a la vez, es por ello que se consideran pluriofensivos. No solo se relacionan al daño económico, sino que también a la intimidad, privacidad, honor, reputación, integridad o normal desarrollo sexual de los menores.

La conjugación de todos estos aspectos tiene repercusión a la hora de la investigación penal ya que se necesita que las fuerzas de seguridad encargadas de dichas tareas tengan conocimientos técnicos mínimos para poder llevar adelante una investigación eficaz. Otro tipo de desafío que presenta este tipo es la cooperación de empresas privadas y proveedores de tecnología de información y comunicación.

El Dr. Julio Téllevez Valdés[5] establece ciertas características principales:

a. Son conductas de cuello blanco (White collar crime) ya que solo un determinado número de personas con ciertos conocimientos avanzados puede cometerlos y en ciertos casos, realizados por profesionales. Sin embargo, en la actualidad esta categoría no resulta ser de todo exacta ya que ha quedado atrasada en el tiempo debido a la evolución en la materia de informática es cada vez más accesible y difundida.
b. Son acciones ocupaciones porque muchas veces se realizan cuando la persona se halla trabajando.
c. Son de oportunidad porque se aprovecha la ocasión propicia para delinquir.
d. Provocan pérdida económicas.
e. Ofrecen posibilidad de tiempo y espacio, se pueden llegar a consumar sin necesidad de presencia física. La transnacionalidad le permite al delincuente encontrarse físicamente alejada de la víctima.
f. Las bandas organizadas suelen actuar en determinados países provocando que las investigaciones sean más complejas ya sea por falta de legislación, materia de cooperación internacional o complicaciones con el idioma.
g. Por su carácter técnico, presentan dificultades para su comprobación.
h. Tienen alto grado de impunidad debido a las pocas denuncias y falta de regulación.
i. Tienden a proliferar cada vez más rápido.

[5] Téllez Valdés, Julio: “Derecho informático” - 4ª ed. - Ed. Mc Graw Hill - México - 2004 - pág. 188-189

3. Sujetos intervinientes

3.1 **Sujeto activo**:

Podemos definir al sujeto activo como una persona física que comete el ilícito en agravio del sujeto pasivo o de la víctima. No obstante, un precedente del año 2001 en Estados Unidos llamado "Napster" penalizó a una persona jurídica, la Corte de Apelaciones de San Francisco responsabilizó indirectamente a la empresa por violar los derechos de autor.

Usualmente se los denomina como "Hackers" "delincuentes silenciosos o tecnológicos" a aquellas personas dedicadas por ficción u otro interés a violar programas y sistemas impenetrables.

Existen otras clases como por ejemplo, "Cracker" a quienes se introducen en sistemas remotos para la destrucción de datos, denegar el servicio a usuarios legítimos y causar problemas; "Phreaker" especialista en telefonía celular; "Lammers" este tipo de delincuente aprovecha el conocimiento adquirido y publicado por expertos.

Aunque estos tipos de sujetos requieren de un conocimiento especial en la materia, la masificación de los servicios informáticos puede navegar en el ciberespacio y obtener herramientas sofisticadas de programación para cometer los actos.

3.2 **Sujeto pasivo**:

Se trata de las víctima sobre la cual recae la conducta reprochada de acción u omisión que pueden ser cualquier tipo de usuario, prestador de servicios, instituciones, órganos estatales, etc. Muchas veces, estos delitos son desconocidos por las víctimas porque no son descubiertos o denunciados provocando que sea difícil su investigación.

El sujeto pasivo puede adoptar una posición neutral sin favorecer ni perjudicar la conducta del delincuente, empero tiene un rol determinante ya que son los únicos que pueden brindar la información a las autoridades para poder descubrir al autor. Existe también una victimización masiva como por ejemplo, la propagación de virus que afecta a un número indeterminado de personas.

4. Bien jurídico protegido

La protección del bien jurídico se hace desde la perspectiva de los delitos tradicionales, con una re- interpretación teleológica de los tipos penales existentes para así poder subsanar las laguna originadas por los avances tecnológicos. Este sector doctrinario entiende que serán los mismos bienes jurídicos que se han actualizado los tipos penales incluyendo nuevos medios de comisión para facilitar su persecución.

Por otra parte, hay quienes consideran que hay un nuevo bien jurídico para proteger que es la información siendo de tal importancia que debe ser tratado de manera independiente de otros

bienes jurídicos. En esta postura encontramos al Dr. Santiago Acurio Del Pino, *"Podemos decir que el bien jurídico protegido en general es la información, pero está considerada en diferentes formas, ya sea como un valor económico, como un valor intrínseco de la persona, por su fluidez y tráfico jurídico, y finalmente por los sistemas que la procesan o automatizan … Por tanto el bien jurídico protegido, acoge a la confidencialidad, integridad, disponibilidad de la información y de los sistemas informáticos donde esta se almacena o transfiere*"[6].

La falta de consenso sobre el bien jurídico protegido en los delitos informáticos arriba en problemas de la aplicación de los tipos penales. Podemos concluir que el bien jurídico en general es la información, pero considerada de distintas formas ya que a través de la misma se puede ver afectados otros bienes como el derecho a la intimidad de una persona, el patrimonio, la propiedad, etc.

[6] Acurio del Pino, Santiago: "Generalidades de los delitos informáticos" – Recuperado de: oas.org

CAPÍTULO II: Clasificación de los delitos informáticos

Al no existir un numerus clausus de los delitos informáticos resulta complicado realizar una clasificación clara y sencilla. En este punto cumple un rol importante el Convenio de Ciberdelincuencia de Budapest ya que es el único instrumento internacional que abarca las áreas relevantes sobre la legislación de la ciberdelincuencia desde un punto del Derecho Penal, Derecho Procesal y Cooperación Internacional.

1. **Delitos contra la confidencialidad, la integridad y la disponibilidad de los actos y sistemas informáticos.**
   1.1 Acceso ilícito: acceso mediante el cual se infringen las normas de seguridad con la intención de obtener información de manera ilegítima.
   1.2 Intercepción ilícita: interpretación mediante medios técnicos de datos informáticos comunicados en transmisiones no públicas efectuada a un sistema ilegítimo de manera deliberada e ilegítima.
   1.3 Interferencia de datos: actos que impliquen daños, que borren, deterioren o supriman datos informáticos.
   1.4 Interferencia de sistemas: actos que obstaculicen el normal funcionamientos de los sistemas informáticos.
   1.5 Abuso de dispositivos e instrumentos técnicos: producción, venta u obtención para la utilización, importación, difusión y otra forma de puesta a disposición de un dispositivo.

2. **Delitos informáticos**
   2.1 Falsedad informática: introducción, alteración, borrado o supresión de datos informáticos que dé lugar a datos no auténticos con la intención de utilizarlos como si fuesen auténticos de manera deliberada e ilegítima.
   2.2 Estafa informática: introducción, alteración, borrado o supresión indebida de datos informáticos y la posterior interferencia en el funcionamiento de un sistema informático cuyo resultado sea la transferencia no consentida de un activo patrimonial en perjuicio de tercero.

3. **Delitos relacionados con el contenido**.
   3.1 Relacionados con la pornografía infantil: reproducción de pornografía infantil con vista a su difusión a través de un sistema informático.

4. **Delitos relacionados con infracciones de la propiedad intelectual y derecho a fines.** Atentados contra la propiedad intelectual, obras literarias y artísticas.

Otras clasificaciones

5. **Según el uso de la red.**
   5.1 Espionaje: relacionado a lo comercial o industrial, consiste en la extracción la información contable de las empresas y cartera de direcciones de clientes corporativas de los discos rígidos de las computadoras, robo de diskettes, copia directa de la información o absorción de las emisiones electromagnéticas que irradia toda computadora.
   5.2 Terrorismo: actos tendientes a desestabilizar un Estado o aplicar presión en el gobierno, utilizando métodos clasificados dentro de los tipos de los delitos informáticos-
   5.3 Narcotráfico

El Dr. Téllez Valdés los clasifica según el uso de sistema operativo. Por un lado como instrumento o medio mediante el cual se valen de computadoras como método, medios y/o símbolos para cometer el delito por ejemplo, falsificación de documentos computarizados, variación de activos y pasivos en la situación contable de las empresas, lectura y sustracción de información confidencial, planeamiento y simulación de delitos convencionales, modificación de datos, desvío de pequeñas cantidades de dinero, alteración del funcionamiento de sistemas, acceso a información no autorizada, intervención de líneas de comunicación, entre otros.

Por otro lado, se puede clasificar como fin u objetivo el cual enmarca las conductas criminales dirigidas contras las computadoras, sus accesorios y programas como el bloqueo total o destrucción de un sistema, daño en los dispositivos de almacenamiento, sabotaje político o terrorismo donde surge un apoderamiento de los centro computarizados o secuestro de soportes magnéticos en los que figure información con fines de chantaje a cambio de un pago de un rescate.

CAPÍTULO III: Investigación forense sobre los medios digitales y la problemática probatoria.

El inconveniente de esta clase de delitos y la complejidad de su investigación y prevención a nivel nacional e internacional configuran una amenazada tanto para el Estado como los ciudadanos que se ven afectados por las conductas que dañan los bienes jurídicos.

Con los avances de la informática y de las telecomunicaciones, los delitos históricos han pasado a convertirse en ciberdelitos ya que implican normalmente el uso de algún elemento digital como un celular, computadora o redes sociales. Conforme a la evolución han surgidos nuevos métodos para investigarlos, para poder valorar el hecho, cómo pasó y poder determinar el autor.

Así es como empieza a surgir la informática forense con el objetivo fundamental de dar respuesta a estos fenómenos, poder identificar, preservar, analizar y presentar datos que resulten válidos en la investigación durante el proceso legal que incluyen la reconstrucción de un bien informático, examinar datos residuales, autenticar datos, explicar las características técnicas del uso aplicado a los datos y bienes informáticos para obtener la evidencia digital.

Las pericias informáticas pueden realizarse sobre cualquier hecho informático, correos electrónicos, páginas web, redes sociales, celulares, computadoras, base de datos, etc. A grandes rasgos la podemos dividir en dos etapas: la recolección y el análisis de la evidencia.

Si bien no existe una definición normativa sobre el concepto de evidencia digital, los diversos organismos internacionales formularon propuestas tomando en cuenta sus características. La Guía de Prueba Electrónica del Consejo de Europa la define como "*La prueba electrónica es aquella información o datos que han sido creados, almacenados o transmitidos a través de dispositivos electrónicos y tienen relevancia en un procedimiento judicial*"[7].

La Organización Internacional de Evidencia Computacional (IOCE) delimitó a la evidencia digital como *"toda información generada, almacenada o transmitida a través de medios electrónicos que puede ser utilizado en una corte judicial*"[8].

[7] Data Protection and Cybercrime División del Consejo de Europa, Guía de Prueba Electrónica. Guía básica para Fuerzas y Cuerpos de Seguridad, Jueces y Fiscales, versión en español, Estrasburgo, Francia, marzo del 2013.

[8] International Organization on Computer Evidence, organización internacional creada ya en 1998 con la finalidad de nuclear a agencias de persecución penal de diferentes países a fin de que intercambien información y buenas prácticas en materia de persecución de delitos informáticos y adquisición de evidencia digital. Recuperado de: http://www.ioce.org/

La evidencia digital es un tipo de evidencia electrónica (concepto más amplio), aunque muchas veces son utilizadas como sinónimos. La evidencia electrónica incluye fotos, audios o videos que puedan ser digitalizados y asumir formatos digitales aunque en su origen no lo eran.

Esta se caracteriza por su alto grado de volatilidad, lo que conlleva por su propia naturaleza que sea frágil, fácil de alterar, dañar o destruir. Resulta imperativo tomar recaudos especiales, ya que de lo contrario podría tornarse inválida a los fines judiciales o ser imprecisa a efectos de esclarecer los hechos.

Tiene carácter técnico ya que no es visible para las personas sin conocimientos y formación especial, de manera tal que requiere algún tipo de traducción tecnológica del formato digital para ser utilizada por los operadores jurídicos.

Puede copiarse sin límites. Si el procedimiento se efectúa correctamente con los instrumentos necesarios estaríamos frente a un clonado y no una simple copia, ya que mantendría todas las características del original. El contenido puede duplicarse infinitas veces y ser exactamente igual al contenido original, lo que le permite realizar múltiples copias exactas para ser distribuidas y analizadas por distintos especialista al mismo tiempo.

Al momento de la recolección y para poder asegurar su integridad, el investigador debe procurar no modificar la información contenida basándose en tres principios. El primero es la adquisición que consiste en que no se debe alterar el archivo de origen. El segundo es la autenticación estableciendo que no se debe verificar que el archivo de evidencia adquirido es igual al archivo de origen y realizar una copia del archivo de evidencia para trabajar sobre el mismo. Y por último, el análisis de los archivos de evidencia se debe realizar sin alterarlos.

Inmediatamente después de estar en contacto con la evidencia es necesario cumplir con la cadena de custodia, entendida como un conjunto de medidas que deben adoptarse con el fin de preservar la identidad e integridad de objetos o muestras que puedan ser fuente de prueba de hechos criminales para su total eficacia procesal.

Se debe:

- Resguardar, documentar, inventariar y etiquetar, resguardar los medios magnéticos en bolsas antiestáticas;
- Transportar la evidencia fuera de medios magnéticos alejada del calor o frío y de lugares con extrema humedad y;
- Evitar durante el transporte choques o vibraciones de los elementos para posteriormente almacenar estableciendo el personal capacitada para su posterior análisis.

Para la recolección se debe tener en cuenta ante qué tipo de evidencia se encuentra (evidencia digital de almacenamiento, evidencia digital de memoria RAM o evidencia digital de tráfico). Este procedimiento en la escena del hecho resulta complejo debido a que se requiere de herramientas forenses, discos rígidos para el almacenamientos de las imágenes y personal capacitado.

La actuación policial basada en la inteligencia y ciberpatrullaje permite a las agencias de aplicación de la ley contar con los elementos para realizar las investigaciones y juzgamientos mediante la geolocalización de equipos a través de la localización remota de GPS o del empleo de detección de antenas utilizada por el dispositivo electrónico. Las direcciones de IP resultan un factor esencial para la determinación de la autoría en caso de cibercriminalidad.

Luego se procede al análisis, constituido por un conjunto de tareas ha realizar para confirmar o refutar la situación que se plantea. Se deben seguir reglas de la buena práctica y protocolos cuando los hubiera. En caso de ausencia de estos existen normas internacionales y procedimientos avalados por instituciones mundialmente reconocidas en la práctica forense informática que establecen pautas para seguir.

Cada persona que interactúe con la evidencia digital debe controlar que el eslabón de la cadena de custodia previo a tomar contacto con la misma y asegurar el último eslabón bajo su control a los efectos de limitar su responsabilidad en el intervalo de su actuación[9].

Sin embargo, resulta imprescindible la sanción de una ley que regule la obtención, almacenamiento y conservación de la prueba digital para unificar criterios y para la viabilidad a largo plazo de las investigaciones. El Código Penal de la Nación tuvo en consideración el Convenio sobre la Ciberdelincuencia de Budapest pero sólo se limitó al Derecho Penal Sustantivo previsto en el Capítulo II “Medidas que deberán adoptarse a nivel nacional” Sección 1 “Derecho Penal Sustantivo”.

No se adhirió a nuestra legislación la sección dedicada al Derecho Procesal Penal, en consecuencia no se adoptaron medidas legislativas que permiten determinar procedimientos penales específicos para la obtención de prueba electrónica de los delitos cometidos por medio de un sistema informático o una legislación que prevea la conservación rápida de datos informáticos almacenados, entendida como la recogida, almacenamiento, retención, reproducción, presentación y valoración de la prueba electrónica.

[9] Delbono, Patricia M. “Cibercrimen y delitos informáticos” (2018). Editorial: ERRIUR

A pesar de las reformas introducidas en el articulado de nuestra ley penal tampoco introdujeron evoluciones que permita contar con reglas específicas para la información relacionada con las TIC.

Nuestro país recepta la aplicación del principio de la libertad probatoria, empero, no existen reglas procesales sobre la admisibilidad, descubrimiento, revelación o valoración de las pruebas relacionadas con la tecnología.

Para dotar a la prueba de seguridad necesaria sin contaminación, pérdida de cadena de seguridad, inalterabilidad, etc., se recurre a peritos oficiales en la etapa de juicio a pedido de partes y con el control como cualquier otro tipo de prueba.

En noviembre del 2020 el Ministerio Público Fiscal actualizó su "Guía de Buenas Prácticas para Obtener Evidencia Electrónica en el Extranjero", la herramienta fue elaborada por la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI) y la Dirección General de Cooperación Regional e Internacional (DIGCRI) con el objetivo de brindar a los investigadoras una herramienta que sirva en caso de que necesiten recabar información digital almacenadas en cuentas y servidores alojados en el extranjero, en particular Estados Unidos y la Unión Europea.

El documento revisa las diferentes clases de información, forma de obtenerla, brinda recomendaciones para su correcta y rápida preservación, medidas previas a solicitar los datos digitales específicos, cómo proceder en casos de emergencia y consejos para organizar el trabajo fiscal antes de enviar solicitudes de cooperación internacional o de asistencia jurídica internacional

Las pautas de la guía se centran en la preservación y obtención de evidencia electrónica almacenada por los proveedores de servicios y no en la obtención en tiempo real de las comunicaciones. Por ejemplo, concentran el análisis de la información almacenada relacionada a las cuentas de correo electrónico y redes sociales como datos del usuario, historial de conexiones, contenidos de los mensajes y otros servicios de internet como registros de nombres de dominio o alojamiento de sitos webs.[10].

La problemática probatoria

En el Derecho Penal y en el Derecho Procesal Penal rige el principio de libertad probatoria, el cual permite que los hechos investigados puedan acreditarse recurriendo a todo tipo de elementos de convicción y prueba que no estén previsto expresamente. A diferencia del Derecho Privado, en el Derecho Penal podemos recurrir a este principio. Esto les permite a los tribunales en el proceso

[10] https://www.fiscales.gob.ar/ciberdelincuencia/el-mpf-actualizo-su-guia-de-buenas-practicas-para-obtener-evidencia-electronica-en-el-extranjero/

penal utilizar medios de investigación y prueba mediante la incorporación de elementos de prueba digital obtenidos.

Sin embargo, no es absoluto y existen excepciones referidas a las limitaciones de origen constitucional basada en la protección de las personas en un Estado de Derecho por razón de su dignidad. Las pruebas obtenidas no pueden estar en violación de las garantías constitucionales o prohibidas por la ley. De esta manera el Estado no puede utilizar libremente los medios probatorios para hacer cualquier cosa en la búsqueda de la verdad, justificándose por la gravedad del ilícito.

El principio *nulla coactio sine lege* determina que todos aquellos actos de investigación, procedimiento probatorios o medios de prueba que impliquen algún grado de coerción o de injerencia[11] de los derechos fundamentales consagrados en la Ley Fundamental o los Tratados Internacionales de Derechos Humanos con jerarquía constitucional deben estar previstos en las leyes.

Esto significa que todas las actividades del Estado, dentro de ellas la actividad probatoria en el proceso penal, que impliquen injerencia de los derechos fundamentales de las personas tienen condición de validez la autorización legal previa.

Suerio establece en su libro *"si bien a la fecha no se ha realizado una reforma en materia de criminalidad informática a nivel del Código Procesal Penal de la Nación, lo cierto es que cada vez más ella resulta imperiosa, indispensable y necesaria, debido al desplazamiento gradual en los procesos penales, de la prueba física, corpórea o tangible hacia la prueba digital, electrónica o intangible".* [12]

Estas nuevas modalidades investigativas van evolucionando conforme a las nuevas modalidades delictivas donde las tareas de investigación pasan a ser "ciberpatrullaje" obligando a los operadores jurídicos estar a la altura día a día. También debemos destacar que la utilización de correos electrónicos, fotografías y servicios de localización sirven como pruebas cruciales para el descubrimiento de ciberdelitos.

En el año 2016 el Ministerio de Justicia y de Derechos Humanos estableció el "Programa Nacional contra la Criminalidad Informática" a fin de esclarecer respuestas a las nuevas modalidades

[11] La injerencia de carácter general modernamente se refiere a todo acto u omisión estatal que de cualquier manera afecta a un derecho fundamental, sea a través de un acto jurídico o una actuación u omisión meramente fáctica; a través de un acto jurídico imperativo o meramente declarativo; con o sin la finalidad de afectar el derecho de que se trate; a través de una afectación directa, mediata o inmediata, cfr. Pérez Barberá, Gabriel, Reserva de ley, principio de legalidad y proceso penal. Recuperado de: http://www.pensamientopenal.com.ar/system/files/2015/12/doctrina42610.pdf.

[12] Sueiro, Carlos C.: "Casos de criminalidad informática y prueba digital" - Ed. Ad-Hoc - 2017 - pág. 21

delictivas mediante el uso de la tecnología, como así también para los delitos trasnacionales potenciados por las TICS, el terrorismo, la trata de personas, el narcotráfico, el lavado de activos, entre otros

Esta nueva herramienta resulta un objetivo fundamental para el sistema de justicia penal que brinda los elementos necesarios para un investigación eficiente y al mismo tiempo, garantizar que las nuevas herramientas de investigación no impliquen un menoscabo para las garantías individuales de los ciudadanos, contar con un Comité Consultivo con especialistas en la temática y presentar anualmente un plan de actividades que tengan en cuenta posibles reformas que resulten necesarias en la legislación penal y procesal penal, proyectos normativos de cooperación judicial entre la Nación y las provincias para mejorar la eficacia en la persecución de los delitos informáticos y cooperación interjurisdiccional en la obtención de evidencia digital, capacitación de operadores, coordinar acciones con organismos nacionales e internaciones, entre el sector público y privado para mejor las investigaciones que involucren la obtención de evidencia digital y la participación de la República Argentina en Foros Internaciones[13].

Pese a ello, las transformaciones que produce el avance tecnológico de información y comunicación usadas por los autores de los delitos son mucho más rápidas que los procesos legislativos de creación y sanción de leyes, de manera tal que cuando el proyecto sea redactado y sancionado quede obsoleto en relación a la tipificación del delito que se busca castigar. Asimismo, debemos contemplar que una vez sancionada la normativa se deben capacitar a los operadores para que la misma sea eficiente y puesta en práctica.

Por medio de la Corte Suprema de Justicia de la Nación el Poder Judicial llevo a efecto actualizaciones en materia de infraestructura tecnológica y capacitación de personas. El Ministerio Público Fiscal ha instaurado el rol de Fiscal en Cibercrimen en el marco de la Procuración General de la Nación respaldado por la División de Delitos Tecnológicos de la Policía Federal de la Argentina, aunque al presente no existan tribunales especializados en la de criminalidad informática.

Al mismo tiempo, el Ministerio Público de Defensa posee cantidad de comisiones y programas, y un gran Departamento de Informática dentro del área de Dirección General pero ninguno para la especialización en la materia[14].

Otro inconveniente que surge es en el ámbito privado, las empresas no se encuentran obligadas por ley a la conservación de información o datos, y ante un requerimiento judicial suelen

[13] http://www.saij.gob.ar/creacion-programa-nacional-contra-criminalidad-informatica-orbita-ministerio-justicia-creacion-programa-nacional-contra-criminalidad-informatica-orbita-ministerio-justicia-nv14027-2016-03-11/123456789-0abc-720-41ti-lpssedadevon

[14] Delbono, Patricia M. “Cibercrimen y delitos informáticos” (2018) Editorial: ERRIUR

proporcionar información los proveedores de internet (por ejemplo, Fibertel), los servidores de correos electrónicos (Hotmail, Gmail), los motores de búsqueda (Google, Yahoo!) y las redes sociales (Facebook, MySpace, etcétera). Es complejo obligar a las empresas de telecomunicaciones o proveedores de servicios a compartir los datos ya que la mayoría de ellas son transnacionales resultando casi imposible aplicar medidas coercitivas o sanciones, además de que cuentan con sus propias políticas de privacidad.

Sin perjuicio de los avances llevados resulta eficaz llevar a cabo la coordinación de un programa con eje central a los desafíos que se plantean y que provea lo necesario para que el Estado pueda dar una respuesta favorable a estos retos, participar en foros internacionales y Convenciones para poder insertarse en los mecanismo de cooperación internacional en la materia y brindar herramientas legislativas.

CAPÍTULO IV: Análisis legislativo en el Derecho Argentino de los delitos informáticos.

En el transcurso del tiempo, nuestra legislación ha adoptado paulatinamente normativas ante el devenir de los delitos informáticos entre las que podemos encontrar la Ley de Piratería (N° 25.036), Ley de Protección de Datos Personales (N°25.326), Ley de Delitos informáticos (N° 26.388), Ley de Despenalización de Calumnias e Injurias (N° 26.551) y el Código Civil y Comercial de la Nación desarrollando su regulación principalmente dentro del área contractual.

1. **Ley de Delitos informáticos (N° 26.388)**

En el Congreso de la Nación se debatieron diversos proyectos en el ámbito de las comisiones de Justicia y Asuntos Penales y de Sistemas, Medios de Comunicación y Libertad de Expresión para el dictado de una ley que abarque todo aquello que se relaciona a la problemática de las ilicitudes informáticas y tecnológicas.

Su sanción en el año 2008 produjo cambios en el Código Penal, teniendo en cuenta el "criterio desconcentrado" no se encuentra un solo bien jurídico amparado, sino que abarca varios en pos de necesidad de tutelar varios bienes jurídicos actuando de manera armoniosa con el Convenio sobre Cibercriminalidad de Budapest.

La Ley incorporando términos al Código Penal a la hora de abordar los delitos informáticos, expresando:

ARTICULO 1º — Incorpórense como últimos párrafos del artículo 77 del Código Penal, los siguientes:

El término "documento" comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión.

Los términos "firma" y "suscripción" comprenden la firma digital, la creación de una firma digital o firmar digitalmente.

Los términos "instrumento privado" y "certificado" comprenden el documento digital firmado digitalmente.

Los documentos en soporte magnéticos tienen una noción mucho más amplía que los documentos manuscritos en soporte papel. Cuando nos referimos a documentos informáticos o electrónicos se apunta a casos en que el leguaje magnético constituye la acreditación, materialización o documentos de una voluntad y donde la actividad de una computadora o de una red únicamente comprueban y/o consignan un hecho, una relación jurídica o una regulación de intereses preexistentes en forma electrónica, digital o magnética. En otras palabras, estas poseen

una característica única que sólo pueden ser leídos o conocidos por el hombre a través de los sistemas o dispositivos traductores que hacen comprensibles las señales digitales.

Este debe entenderse como toda expresión en lenguaje natural o convencional y cualquier expresión gráfica, sonora o en imagen, recogidas en cualquier soporte material e incluso en soportes informáticos con eficacia probatoria o con cualquier otro tipo de relevancia jurídica.

Desde la perspectiva del derecho comparado existen diversas conceptualizaciones del término documento:

En México el documento electrónico o informático se concibe como un medio de expresión de la voluntad con efectos de creación, modificación o extinción de derechos y obligaciones por medio de la electrónica, informática y telemática[15].

La legislación española establece un concepto de documento electrónico que queda incorporado a la noción genérica de documento por cuanto define al documento como todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier tipo de relevancia jurídica[16].

Los conceptos de “firma” y “suscripción” comprenden la firma digital, la creación de una firma digital o una firma digitalmente. Los “instrumentos privados” y “certificado” comprende el documento firma digitalmente.

Como consecuente al Protocolo Relativo a la Venta de Niños, la Prostitución Infantil y la Utilización de los Niños en la Pornografía de la ONU de 1989 se sustituyó el Artículo 128 del Código Penal- Delitos contra la integridad sexual, figuras y conductas orientadas a la indemnidad sexual de los menores de 18 años en el que se sancionan las conductas típicas que consuman el delito tendientes a producir, financiar, ofrecer, comerciar, publicitar, facilitar, divulgar o distribuir material pornográfico. Se consagra un delito de acción, de resultado instantáneo con pluralidad de actos y que basta cualquier conducta tipificada para que cause el resultado típico.

El objeto material es la representación ya sea por dibujos, imágenes, fotografías, etc. que se apoyan en soporte físico informático, el tipo subjetivo es doloso admitiendo el eventual donde el sujeto activo puede ser cualquier persona, mientras que el sujeto pasivo debe ser una persona menor de 18 años. Es admisible la tentativa.

[15] Documento electrónico. Unidad de Apoyo para el Aprendizaje. Recuperado de: http://132.248.48.64/repositorio/moodle/pluginfile.php/1011/mod_resource/content/4/contenido/index.html#:~:text=Por%20lo%20tanto%2C%20el%20documento,a%20trav%C3%A9s%20las%20se%C3%B1ales%20digitales.

Al mismo tiempo, se sanciona el comportamiento típico de quien facilitare el acceso a espectáculo o suministrare material pornográfico en que participen menores de 18 años prevista en la Ley N° 25.087 modificatoria del Código Penal en lo relativo a los delitos contra la integridad sexual.

Reprime el comportamiento típico de tener en su poder representaciones de las descriptas anteriormente, constituyendo un delito de tenencia de objetos bajo el poder del agente. El objeto material son las representaciones de los menores de 18 años utilizando soportes físicos o en uno magnético mediante dolo directo. La figura por su carácter no admite la tentativa.

El último párrafo del Artículo 2 relaciona las mismas conductas pero con menores de 14 años.

Otra modificación relevante que introduce la ley es la sustitución del epígrafe del Capítulo III del Título V del Libro II del Código Penal- Violación de Secretos y de la Privacidad que incluye la privacidad como bien jurídico protegido defendiendo el bien jurídico libertad.

A pesar de que ciertos juristas relacionan los términos "intimidad y privacidad", son dos conceptos que merece ser diferenciados. Carlos S. Nino (2010) resalta que *" el bien de la privacidad se relaciona con el derecho que tienen los ciudadanos a que no se los moleste por las acciones voluntarias que no afectan a terceros"*[17].

En el caso "Ponzetti de Balbín" (1984)[18] la Corte Suprema de Justicia de la Nación implícitamente equipara la intimidad y la privacidad, sin embargo posteriormente en el caso "Baldivieso" (2010) expresa que deben distinguirse los conceptos de intimidad y privacidad[19].

En lo concerniente a los correos electrónicos, anteriormente a la sanción de la Ley N° 26.388 no estaba equiparada por lo que todas las conductas que se planteaban judicialmente eran rechazadas por inexistencia de delitos. La comunicación electrónica debe entenderse como todo mensaje enviado por un remitente a un destinatario a través de un sistema electrónico como correo electrónico, chat, fax, SMS, etc.

En el fallo "Lanata" (1999)[20] las acciones realizadas sobre correos electrónicos eran consideradas atípicas al no encontrarse específicamente incluidos en el Código Penal. Posteriormente la Cámara Nacional de Apelaciones en lo Criminal y Correccional dispuso: *"Queda claro que el "e-mail" es un medio idóneo, certero y veloz para enviar y recibir todo tipo de mensajes,*

[17] Nino, C.S. (2000). *Fundamentos de derecho constitucional. Análisis filosófico, jurídico y politólogo de la práctica constitucional.* (1ª Ed., lª Reimpresión). (Tº V p. 304). Buenos Aires: Astrea.
[18] CSJN. Fallo 306:1892. "Ponzetti de Balbín, Indalia c/Editorial Atlántida S.A.". Buenos Aires, 1984.
[19] CSJN. "Baldivieso, César Alejandro s/Causa Nº 4733", 2010.
[20] CNCC "Lanata, Jorge s/Excepción de Falta de Acción". Buenos Aires, 1999.

misivas, fotografías, archivos completos, etc.; es decir, amplía la gama de posibilidades que brindaba el correo tradicional al usuario que tenga acceso al nuevo sistema. Es más, el correo electrónico posee características de protección de la privacidad más acentuadas que la inveterada vía postal a la que estábamos acostumbrados, ya que para su funcionamiento se requiere un prestador del servicio, el nombre de un usuario y un código de acceso que impide a terceros extraños la intromisión en los datos que a través del mismo puedan emitirse o archivarse.

En tal sentido, la correspondencia y todo lo que por su conducto pueda ser transmitido o receptado, goza de la misma protección que quiso darle el legislador al incluir los artículos 153 al 155 en la época de la redacción del código sustantivo, es decir, como cuando aún no existían estos avances tecnológicos".

La incorporación del Artículo 153 bis del acceso ilegítimo a un sistema informático posee dos aspectos; la exclusividad y la intimidad. El objeto material recae sobre el sistema o dato informático de acceso restringido y acceder a él es la conducta típica siendo un delito de acción de resultado instantáneo. Se requiere que el dolo sea directo por conocer el acceso ilegítimo donde los sujetos activos y pasivos pueden ser cualquier persona.

El Artículo 6 sustituye en 155 del Código Penal actualizando el delito de publicación indebida por publicaciones electrónicas dentro de los objetos materiales del delito. El ataque que se produciría al bien jurídico es un peligro hipotético o potencial. La figura consiste en la acción de publicar indebidamente donde se incluye una exclusión de responsabilidad penal para quien obre con el propósito inequívoco de proteger el interés público entendida como de utilidad para todos los habitantes, de todo un país o de una comunidad regionalmente determinada.

De igual manera, la sustitución del Artículo 157 introdujo el término dato y proteger penalmente la información en poder de la Administración Pública por su prohibición de ser reveladas a terceros y su carácter de ser secreta. Las conductas típicas comprenden descubrir, manifestar o dar a conocer representaciones de hechos, manifestaciones o conceptos secretos, contenidos en un formato físico o magnético.

La norma deroga el Artículo 177 bis inc. 1 del Código Penal y por otro lado sustituye el Artículo 157, se trata de la conducta dolosa de quien accediere a una banco de datos personales de manera no autorizada, siendo el sujeto pasivo el dueño o titular de la base de datos y quien tenga la responsabilidad de proteger y resguardar los datos. El sujeto activo puede ser cualquier persona y se agrava en el caso de que el sujeto sea un funcionario público.

Se incorpora el inc. 16 del Artículo 173 del Código Penal la figura de Estafa Informática-Fraude Informático. Es un delito que requiere dolo directo, es de resultando instantáneo cometido

por acción u omisión cunado el sujeto activo ocupa un posición de garante que lo responsabiliza. El fraude informático se diferencia de la estafa tradicional ya que no exige engaño y error, igualmente no se trata de una disposición consentida.

A fin de subsanar el vacío legal en cuanto a la informático y los daños que su uso podía ocasionar -sabotaje informático o cracking-, se añade al Artículo 183 del CP las conductas de alterar, destruir o inutilizar datos, documentos, programas o sistemas informáticos y quien utilizare cualquier programa destinado a causar daños en los sistemas informáticos. El delito se materializa con la utilización de virus informáticos, caballos de troya, gusanos, bombas lógicas, etc.

El delito de daño informático se agrava cuando se ejecuten en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de previsión o de transporte de energía, medios de transporte u otro servicio público. La calidad de público debe entenderse con la naturaleza de la información y la titularidad estatal.

La sustitución del Artículo 197 del CP- Delitos contra la seguridad del tránsito y de los medios de transporte y comunicación implica una ampliación de los objetos materiales del delito abarcando las comunicaciones públicas y privadas. La Ley de Delitos informáticos incorpora a la norma la comunicación “de otra naturaleza” de manera tal que no sólo se castiga la interrupción o entorpecimiento de comunicaciones telegráficas o telefónicas, sino cualquier tipo de comunicaciones realizadas por medios informáticos.

El Artículo 255 del Código Penal correspondiente al Título XI Delitos contra la Administración Pública mantuvo su redacción original, al cual la Ley 26.388 incorporó el verbo típico “alterar” y la expresión “en todo o parte” con el fin de incluir todas aquellas formas informáticas tecnológicas de producir una violación de prueba, registros o documentos. También agrego el carácter de “público” al funcionarios y sustituyo la palabra “culpable” por “autor”.

El bien jurídico protegido es la confianza pública que se tiene sobre los medios probatorios, registros y documentos que tiene carácter oficial. La figura tiene como fin proteger a estos objetos destinados a servir como prueba ante una autoridad competente y a los registros o documentos confiados a la custodia de la autoridad o de un particular en interés del servicio público.

El delito se agrava por la calidad del autor cuando este fuese el mismo depositario del objeto destinado a servir la prueba independientemente de que éste sea un particular o un funcionario público. Se deberá aplicar además una pena de inhabilitación especial por el doble de tiempo de la condena la que producirá la privación del empleo, cargo, profesión o derecho y la incapacidad de obtener otro del mismo género. Si el autor fuese funcionario público la inhabilitación especial prevé la pérdida de depositario y la imposibilidad de ocupar cargos públicos en el tiempo de la pena.

Para que la figura sea culposa es necesario una conexión subjetiva entre la conducta negligente o imprudente del depositario y la acción dolosa de un tercero. Cuando se trate de objetos destinados a servir de prueba el autor sólo puede ser el funcionario público depositario. En cambio, si se trata de registros o documentos el sujeto activo podrá ser un funcionario público o un particular.

2. **Otras normativas relacionadas a los delitos informáticos**

Ley de Propiedad intelectual (N° 11.723)

Establece el régimen legal de la propiedad intelectual que abarca las obras científicas, literarias y artísticas, los escritos de toda naturaleza y extensión, entre ellos los programas de computación fuente y objeto[21].

Ley de Piratería de Software (N° 25.036)

Los programas de computación reúnen todos los requisitos para ser considerados como propiedad intelectual contemplado en la Ley de Propiedad Intelectual, pero desde su promulgación se han incorporado cambios tecnológicos como la creación de ordenadores y la incorporación de tecnología, lo que trajo aparejado conductas antijurídicas no siempre contempladas por la ley.

El bien jurídico tutelado de esta nueva normativa consiste en la reproducción sin autorización con o sin fines de lucro de programas de ordenador y compilaciones de datos[22].

Ley de Protección de Datos Personales (N° 25.326)

Posee principios relativos a la protección de datos, desde los derechos de los titulares hasta los usuarios y responsables de archivos, registros y bancos de datos. Con esta ley lo que se pretende resguardar es el derecho al Honor y la Intimidad [23].

Ley de Grooming (N° 26.904)

Esta ley incorpora el Artículo 131 del Código Penal que prescribe: *"Será penado con prisión de seis (6) meses a cuatro (4) años el que, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contactare a una persona*

[21] Recuperado de: http://servicios.infoleg.gob.ar/infolegInternet/anexos/40000-44999/42755/norma.htm

[22] Recuperado de: http://www.saij.gob.ar/adolfo-prunotto-laborde-pirateria-software-nueva-ley-25036-dasf060047/123456789-0abc-defg7400-60fsanirtcod

[23] Recuperado de: http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm

menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma"[24].

Ley 863 de la Legislatura de la CABA

Los establecimientos comerciales dentro de la Ciudad Autónoma de Buenos Aires que brinden acceso a internet deben instalar y activar en las computadoras que estén a disposición del público filtro de contenidos de páginas pornográficas[25].

Instrumentos internacionales y cooperación internacional

En las últimas décadas se realizaron avances considerables en la promulgación de Instrumentos Internacionales. La supresión de los delitos informáticos es una estrategia básica en materia de ciberseguridad y de protección de la infraestructura de la información esencial a través de la adopción de una legislación adecuada, esto implica una responsabilidad compartida por parte de los Estados y exige una acción de coordinación y preparación.

Estos instrumentos constituyen antecedentes en la materia para que los Estados adapten sus normas penales, en otras palabras, tienen relevancia a nivel mundial debido a que sirven como base para elaborar las normativas locales de los países adheridos. Dentro de ellos podemos encontrar:

a. La Organización para la Cooperación y el Desarrollo Económico (OCDE)
b. La Convención contra la Delincuencia Organizada Transnacional
c. El Convenio sobre Criminalidad de Budapest

En 1982 la OCDE inició propuestas para armonizar a nivel internacional el derecho penal vigente para poder abordar el problema que comprende los delitos cibernéticos. Posteriormente publicó un informe llamado "Computer related crime: analysis of the legal policy" ("Delitos de informática: análisis de la normativa jurídica") que analizaba las distintas legislaciones, formuló propuestas para combatir el crimen donde establece una lista mínima de delitos que los países podrían tipificar.

El Consejo de Europa instauró una serie de pautas orientadas a los parlamentos de los países miembros en relación a las conductas punibles donde intervenían los dispositivos informáticos.

[24] Recuperado de: http://servicios.infoleg.gob.ar/infolegInternet/anexos/220000-224999/223586/norma.htm
[25] Recuperado de: http://www.informatica-juridica.com/anexos/legislacion-informatica-de-ley-863-de-proteccion-de-menores-en-establecimientos-comerciales-que-brindan-acceso-a-internet-de-15-de-agosto-de-2002/

Mediante un Comité Especial de Expertos sobre Delitos relacionados con el Empleo de Computadoras se evaluaron temas sobre la prevención del riesgo, represión de delitos, procedimientos de investigación, métodos de confiscación trasnacional y cooperación internacional.

La Convención contra la Delincuencia Organizada Transnacional conocida también como la Convención de Palermo (Italia) adoptada en diciembre del año 2000 surgió a los efectos de la globalización y las nuevas tecnologías con el fin de prevenir y combatir más eficazmente la delincuencia organizada transnacional.

Otro instrumento internacional de gran importancia es el Convenio sobre Criminalidad de la Unión Europea firmado en Budapest en el año 2001, adherido a nuestro país en el año 2017, donde establece directrices generales sobre la tipología de los delitos en el ámbito de la cibercriminalidad, en el ámbito del Derecho Penal y Derecho Penal Procesal, principios de cooperación en materia judicial y procedimientos vinculados a la investigación criminal.

En su preámbulo establece su finalidad: *""prevenir los actos que pongan en peligro la confidencialidad, la integridad y la disponibilidad de los sistemas, redes y datos informáticos…"*, además de evitar que las redes informáticas y la información electrónica sean utilizados como medio para cometer delitos y que las pruebas de las infracciones sean almacenadas y transmitidas por medio de esa redes. [26]

Para cumplir con el propósito dispone que los Estados parte deberán adoptar medidas legislativas y de otro tipo para tipificar los delitos en su derecho interno sobre el acceso deliberado e ilegítimo en todo o parte de un sistema informático, intercepción de datos informáticos en transmisiones no públicas dirigidas a un sistema informático, originadas o efectuadas dentro del mismo; el acceso ilegítimo que dañe, borre, deteriore o suprima datos informáticos, como así también ataques contra su funcionamiento.

Con relación al abuso de dispositivos establece que los Estados deberán tipificar las conductas que comprendan la venta, obtención, importación, difusión u otra forma de puesta a disposición de dispositivos informáticos previstos en el Convenio, de contraseñas, códigos de acceso o datos similares con la intención de cometer algún delito.

Los títulos 2, 3 y 4 detallan los delitos informáticos: falsificación informática, fraude informático, delitos relacionados con el contenidos como aquellos concernientes a la pornografía infantil y delitos relacionados con infracciones de la propiedad intelectual y derechos a fines.

[26] "Convenio sobre la ciberdelincuencia" - Publicación del Consejo de Europa - Estrasburgo - 2001 - Preámbulo

Cada Parte adoptará medidas que responsabilicen a las Personas Jurídicas cuando comentan alguno de estos ilícitos, establecer una responsabilidad penal, civil o administrativa y la imposición de sanciones, medidas penales o no penales, efectivas, proporcionadas, disuasorias y pecuniarias. Para el caso de las personas físicas deberán establecer medidas coercitivas para las conductas previstas y que sus sanciones sean efectivas, proporcionadas y disuasorias, comprometiéndose en todos los casos a establecer procedimientos a los efectos de investigaciones o de procedimientos penales específicos.

Deberán acoger medidas legislativas o de otro tipo para la conservación rápida de datos informáticos almacenados y custodia para ponerlos a disposiciones de la autoridad competente, especialmente cuando aquellos datos sean susceptibles de pérdida o modificación.

Impone que se implementen medidas para ordenar a los proveedores de internet que ofrezcan servicios de comunicación y servicios a que aporten datos como identidad, direcciones postales, situación geográfica, números de teléfono, números de acceso, datos relativos a pagos y facturaciones del contrato o acuerdo de prestación de servicio ante las autoridades competentes.

En lo que respecta a la jurisdicción deberán establecer las medidas pertinentes para afirmar su jurisdicción respecto de cualquier delito previos en el Convenio cuando este se haya cometido: "*a. en su territorio; o b. a bordo de un buque que enarbole su pabellón; o c. a bordo de una aeronave matriculada según sus leyes; o por uno de sus nacionales, si el delito es susceptible de sanción penal en el lugar en que se cometió o si ningún Estado tiene competencia territorial respecto del mismo."*

En materia de Cooperación Internacional ordena que los Estados deben prestarse asistencia mutua a los efectos de las investigaciones y procedimientos de los delitos informáticos, quedando sujetas a la condiciones establecidas en el derecho interno de cada Parte o en los tratados de asistencia mutua aplicables.

El Artículo 35 del Convenio prevé la Red 24/7 el cual prescribe: *"1. Los Estados designarán un punto de contacto localizable las 24 horas del día, y los siete días de la semana, con el fin de asegurar la asistencia inmediata en la investigación de infracciones penales llevadas a cabo a través de sistemas y datos informáticos o en la recogida de pruebas electrónicas de una infracción penal.*

Esta asistencia comprenderá, si lo permite el derecho y la práctica interna, facilitar la aplicación directa de las siguientes medidas:

a. aportación de consejos técnicos;

b. conservación de datos según lo dispuesto en los artículos 29 y 30; y

c. recogida de pruebas, aportación de información de carácter jurídico y localización de sospechosos.

2. a. Un mismo punto de contacto podrá ser coincidente para dos Estados, siguiendo para ello un procedimiento acelerado.

b. Si el punto de contacto designado por un Estado no depende de su autoridad o autoridades responsables de la colaboración internacional o de la extradición, deberá velarse para que ambas autoridades actúen coordinadamente mediante la adopción de un procedimiento acelerado.

3. Los Estados dispondrán de personal formado y dotado a fin de facilitar el funcionamiento de la red".

En nuestro país fue creada por medio la resolución 1291/2019 para asegurar la asistencia inmediata en la investigación de los tipos penales llevados a cabo por medio de sistemas informáticos y datos informáticos o en la recolección de pruebas electrónicas de una infracción penal, exigiendo una respuesta rápida.

Dentro de las funciones deberán prestar asesoramiento técnico en las investigaciones penales en la que los Estado Parte requiere asistencia, colaborar con pedidos de conservación de datos informáticos y facilitar los mecanismos para la obtención de pruebas informáticas respetando el marco normativo, facilitar las comunicaciones, asistir la localización de sospechosos y a los funcionarios del sistema penal. Dicha unidad también tiene como función proveer y requerir a las partes extranjeras asistencia internacional durante el proceso de investigación inicial para preservar la evidencia digital y que posteriormente se encuentre disponible[27].

[27] https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-1291-2019-332246

CAPÍTULO V: Estafas informáticas y su incidencia durante el confinamiento en Argentina.

1. Regulación

Mediante la Ley 25.930 del año 2004 que modificó el Código Penal se reformó el artículo 285 e incorporó el artículo 173 inc. 15 el siguiente: "*El que defraudare mediante el uso de una tarjeta de compra, crédito o débito, cuando la misma hubiere sido falsificada, adulterada, hurtada, robada, perdida u obtenida del legítimo emisor mediante ardid o engaño, o mediante el uso no autorizado de sus datos, aunque lo hiciere por medio de una operación automática*".

Este inciso añade la defraudación por el uso de tarjeta de compras cuando la misma hubiese sido falsificada o adulterada, robada, pérdida, etc. De igual manera, este último artículo prescribe la conducta de "hackeo" como las defraudaciones cometidas por los "Hackers", es decir los piratas informáticos.

El tipo penal consiste en la utilización o uso de datos o información de un sujeto sin que medie autorización, es un ataque a la propiedad que consisten en una disposición patrimonial perjudicial mediante el cual el actor busca un beneficio propio o para un terceros.

Como en las demás defraudaciones, es un delito de resultado que requiere un perjuicio material. El ilícito sólo admite dolo directo estableciendo que el autor debe conocer los datos que obtuvo por un medio ilegal, sin estar autorizado para utilizarlos y que además, los haya obtenido para causar el perjuicio patrimonial. El daño se genera en el momento en que la disposición patrimonial acontece, tratándose de un delito instantáneo y admitiéndose la tentativa.

Es menester enfatizar que dentro de este ámbito desempeña un rol fundamental principio general del derecho penal consagrado en el artículo 18 de la Constitución Nacional el cual prescribe que "*Ningún habitante de la Nación puede ser penado sin juicio previo fundado en ley anterior al hecho del proceso*" ,y la prohibición de aplicar el principio de analogía para castigar una conducta no tipificada en virtud de la existencia de otra conducta semejante. Las normas penales deben estar compuestas por un precepto legal y su respectiva sanción, caracterizándose por ser generales, abstractas, expresas y escritas.

Frente a la necesidad de tipificar las conductas criminales llevadas a cabo a través de medios informáticos, llenando algunos vacíos legales y como medio de prevención y protecciones de los bienes jurídicos se produjo un gran avance a partir de la sanción de la Ley Nacional 26.388.

Se incorporó el nuevo medio de comisión del delito establecido en el Código Penal, como lo realizaron distintos países europeos en los que podemos mencionar España, Italia, Alemania, entre otros[28].

Esta normativa ubica a la Argentina dentro de los estados que tienen en consideración a la omnipresencia de las TIC en la sociedad, el uso diario y su utilización para la comisión de delitos que dañan a las personas y sus bienes, dándole una herramienta a la Justicia al momento de establecer la pena de dichas conductas.

No es una ley especial que regula este tipo de delitos en un legislación separada del Código Penal, con figuras propias y específicas, sino que es una ley modificatoria que a su vez, sustituye e incorpora figuras típicas con el objeto de complementar la regulación de las acciones y los medios de comisión de los delitos previstos en el articulado del Código.

El artículo 9° de la Ley de Delitos informáticos prescribe que se incorpora dentro del Capítulo IV "Estafas y otras defraudaciones" como inciso 16 al artículo 173 del Código Penal el siguiente: "*El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos".*

En este inciso se eliminó la actuación del delincuente sin la autorización del usuario, ya que si se agregaba un elemento al tipo podría resultar innecesario y confuso, pues la autorización no podría prescindir la ilicitud de la conducta predestinada a cometer el delito.

Su incorporación superó la idea clásica de error, ardid, disposición y perjuicio patrimonial que ha causado desacuerdos en la jurisprudencia. La falta de voluntad, discernimiento y la posibilidad de hacer caer en error a una maquina o sistema provocó lagunas de punibilidad destacando la necesidad de un tratamiento legal punitivo por ejemplo, las maniobras realizadas a través de los cajeros automáticos.

No obstante, la aceptación de la defraudación informática como delito en el articulado del Código generó grandes debates donde las opiniones se encontraban divididas. Un gran parte de la Doctrina consideraba que se debían encuadrar la apropiación de bienes informáticos en la figura de

[28] En España se incorporó al Código Penal por medio del artículo 248.2 a), la mayor parte de la Doctrina estima que es un delito de estafa clásico, pero el problema surgía que esta realidad no encuadraba en la verdadera naturaleza del delito siendo necesario la creación de un nuevo delito.
Alemania reguló la estafa informática en el artículo 263a del Código Penal Alemán incorporada mediante la Ley de lucha contra la criminalidad económica, introduciendo un tipo paralelo a la estafa como una necesidad política- criminal debido a la emergente utilización de procesamiento de datos y que los tipos penales no podían comprender tales comportamientos.
Por otro lado, en Italia se encuentra regulado en el artículo 640 ter del Código Penal destinado a reprimir las conductas de enriquecimiento ilícito por el empleo fraudulento de medios informáticos.

defraudación mediante la utilización de medios informáticos y otro sector, consideraba que esta apropiación debería ser considerada como hurto ya que se interpretaba si podía o no la información ser susceptible de apoderamiento ilegítimo mediante el uso de medios informáticos.

En cuando al bien jurídico protegido en términos generales es la propiedad, resultando aplicables las reglas previstas en el artículo 172 del Código Penal. La discusión central actualmente se acentúa en determinar si es verdaderamente el bien jurídico protegido la propiedad, o el patrimonio específicamente.

Un sector doctrinario entiende que es el patrimonio ya que la acción lesiva está dirigida directamente a este y no al componente de la propiedad de la víctima, como en el caso de los delitos de robo y hurto. No sólo incluye acciones que lesionan y ponen en peligro la propiedad, sino que también afectan otros valores patrimoniales como la posesión o el derecho a un crédito[29].

La defraudación informática instaura un novedoso sistema de estafa la cual se lleva a cabo mediante la manipulación de cualquier sistema informático que afecte tanto la propiedad como el patrimonio. Pablo G. Lucero y Alejando A. Kohen en su obra demarcan "*Nos inclinamos por pensar que el bien jurídico protegido es más bien el patrimonio, ya que con la conducta lesiva se afecta holísticamente el patrimonio mismo del damnificado y no un componente de la propiedad de dicho sujeto pasivo, como podría ser el caso de los delitos de hurto o robo*"[30].

Entre las diferentes formas de fraudes podemos encontrar la alteración de registros informáticos, uso no autorizado de tarjetas de débito y crédito, sustracción de datos personales para utilizarlos en sitios web efectuando comprar en línea, phishing, utilización de claves falsas, "caballo de Troya", "técnica del salami/ salchichón", entre otros.

Generalmente los datos son facilitados por las mismas víctimas mediante encuestas, llamadas telefónicas, correo electrónico, robo de documentos y tarjetas, simulación de sorteos, etc. El damnificado toma conocimiento que ha sido víctima del delito cuando recibe una intimación para cancelar las deudas, la notificación de juicio ejecutivos o pedidos de detención.

Los datos por sí mismos no constituyen información, ya que sólo son una representación simbólica, atributo o característica de una identidad. Estos se convierten en información cuando su creador les añade significado siendo fundamental en el campo de la informática. Todos los casos que no puedan ser enmarcados en el inciso 15 del artículo 173 serán incluidos en el incisos 16 del

[29]DONNA, Edgardo; Derecho Penal, Parte Especial, Tomo II-B, Rubinzal-Culzoni Editores, Buenos Aires, 2001, p. 263.
[30] Lucero Pablo. G, Kohen Alejandro A. Delitos Informáticos (2015) Bueno Aires, Argentina. Editorial: Albrematica

mismo artículo ya que la transmisión de datos y manipulación de sistemas informáticos se vincula con las tarjetas, siendo una modalidad propia del primer inciso, mientras que toda operación no vinculadas con estos instrumentos tendrá su adecuación en el siguiente inciso.

En consecuencia, en mayo del 2010 la Dirección Nacional de Protección de Datos Personales de Argentina creó el Centro de Asistencia de las Víctimas de Robo de Identidad con el objetivo de asistir y orientar a las personas víctimas de este delito, poder informar sobre las medidas de prevención y adoptar medidas necesarias para evitar que este medio de estafa avance sobre la sociedad[31].

Desde esta perspectiva el robo de identidad no es visto como un típico delito informático, sino como un medio idóneo para poner llevar a cabo la estafa. Inicialmente el robo de identidad estaba ligado al phishing mediante el cual se engañaba a la víctima para que verifique sus datos personales y bancarios.

Posteriormente, el robo de identidad fue evolucionando, encontrando distintos escenarios. El delincuente no solo accedía a los datos por medio del correo electrónico, sino que también a partir de los robos en la vía pública de los documentos de identidad y tarjetas contando con la información necesaria para cometer los delitos a través de la web y así, cometer delitos mediante medios informáticos.

La Ley de Delitos Informáticos guarda íntima relación con la Ley de Protección de Datos Personales (25.326) al referirse a la protección integral de los datos personales de las personas físicas y jurídicas que se encuentra en archivos, registros, banco de datos y cualquier otro medio técnico de tratamiento de datos ya sean público o privados garantizando el derecho al honor y a la intimidad de las personas, como el acceso a la información.

La formación de archivos de datos será licita cuando se encuentre debidamente inscriptos tal como lo prescribe la ley y reglamentaciones especificas sin que sea contraria a las finalidades de la misma y la moral. La recolección no puede realizarse por medios desleales, fraudulentos o en forma contraria a las disposiciones legales.

Además establece que es necesario el consentimiento libre, expreso e informado del titular para el tratamiento de datos personales y se debe establecer su finalidad para lo que serán tratados. Igualmente prohíbe la posibilidad de que una persona sea obligada a proporcionar datos sensibles.

[31] Dirección Nacional de Protección de Datos Personales, PROTECCION DE LOS DATOS PERSONALES, Disposición 7/2010

Por último, el responsable o usuario de archivos de datos debe adoptar todos las técnicas y medidas necesarias para garantizar la seguridad y confidencialidad evitando la adulteración, pérdida, consulta o tratamiento no autorizado y que permita detectar desviaciones, intencionales o no de información que ponga en riesgo al titular de las mismas. Está prohibida la transferencia de datos personales de cualquier tipo a otros Estados, organismos internacionales o supranacionales que no proporcionen niveles de protección adecuados.

De esta forma se puede concluir que la Ley de Delitos informáticos, el Código Penal y la Ley de Datos Personales forman un sistema armonizado actuando de forma conjunta para la correcta protección de la información evitando la defraudación informática y cualquier otro tipo de delitos en los que sea necesaria esta información.

2. Las estafas en tiempo de pandemia

La libre circulación de navegación, frecuencia de acceso a la red y el uso de información por parte de los usuarios para transferir, difundir y emitir datos como para acceder a ellos por medio de internet les permite al mismo tiempo ser potenciales víctimas como perpetradores de delitos.

Además, facilita la libre comercialización de información tanto en el mercado legal como software, películas, libros como en el mercado negro (Deep web) donde el acceso engañoso a un banco de datos, revelación ilegítima de la información personal, contraseñas y números de tarjetas de crédito/ débito se distribuyen con el propósito de realizar fraudes y robos.

La constante evolución de las TIC (tecnologías de la información y comunicación) desarrolla nuevas técnicas y medios sofisticados con el objetivo de burlar las medidas de seguridad existente y cometer nuevos hechos ilícitos.

La principal fuente de ataques no se centra en sistemas informáticos de computadoras de empresas debido a que por lo general suelen tener mejor protección que los privados, sino a usuarios comunes ya que no cuentan con la protección de los primeros. Las computadoras personales suelen tener información delicada y confidencial como datos de tarjetas de crédito o bancarios con los que el delincuente puede concluir sus actividades delictivas.

Actualmente se han comenzado a utilizar herramientas de tipo software o programas espías que le otorga facilidad para acceder a los datos personales, con la ayuda de los programas instalados previamente el ciberdelincuente puede atacar miles de personas utilizando sólo una computadora.

El método más habitual que se recurre para acceder a los datos es la ingeniería social. Este resulta relevante ya que se caracteriza en la intromisión humana mediante un artificio o ardid para engañar a las personas. El acceso ilícito en este caso consiste en una manipulación a las personas con la finalidad de obtener acceso a la información de una manera más sencilla.

Suele ser un procedimiento poderoso y eficaz dado a que se enfoca en el punto débil de la seguridad informática que reside en la falta de conocimiento de los usuarios. Por ejemplo la estafa informática o también conocido como “phishing” (aludiendo a la pesca de datos) se ha convertido de un delito característico del ciberespacio y que consiste en obtener por medio de fraude información personal haciéndose pasar por una persona o por empresas conocidas a través de comunicaciones electrónicas con apariencia de ser notificaciones oficiales y genuinas.

Luego de obtener los datos el perpetrador suele aplicar una estrategia que consiste en pequeñas pérdidas financieras a cada una de las víctima. Los montos extraídos al ser insignificantes son menos probables de ser detectados y que las personas inviertan su tiempo tratando de rastrear esas transacciones e investigar el delito.

Otro tipos de metodologías que podemos encontrar son el phishing bancario o con tarjetas de créditos como móvil para cometer delitos financieros, compras por portales no válidos, compras a través de redes sociales, compras o validaciones de datos de manera telefónica e incluso por medio de cadenas de mensajes que nos puede enviar por aplicaciones (por ejemplo, WhatsApp).

El tráfico ilícito de información personal, las estafas bancarias, phishing, estafas en plataforma de compra venta y suplantación de identidad si bien ya estaban aumento, tuvieron un gran auge durante al aislamiento social valiéndose de las víctimas que pasan más tiempo conectadas a internet, captando la atención de los cibercriminales y aprovechando los descuidos para vulnerar los sistemas informáticos.

La adopción apresurada de estos hábitos y las faltas de prácticas de seguridad conlleva a distintos tipos de riesgos en línea como las estafas y distribución de información. Desde el comienzo de la pandemia Argentina se ha convertido en el tercer país de América Latina con amenazas digitales.

La Asociación Argentina de Lucha Contra el Cibercrimen (AALCC) ha indicado que el riesgo de los usuarios de PC creció un 27% con relación al 2019; durante la cuarentena se observó un incremento de especialmente en las extorsiones online, phishing y fraude[32].

Actualmente la cifra salto un 116% en comparación al año 2020 de acuerdo al registro de la misma Asociación utilizando las mismas metodologías recibiendo un total de 284 consultas cuando el año pasado habían sido de 131[33]

[32] https://www.cibercrimen.org.ar/2020/08/17/ciberseguridad-una-nueva-prioridad-para-las-organizaciones/
[33] https://www.cibercrimen.org.ar/2021/01/27/las-denuncias-sobre-delitos-informaticos-aumentaron-en-gran-escala-durante-la-pandemia-advierten-la-pagta-local-diario-clarin/

En relación a este tema, en Puerto de Iguazú se registraron una serie de estafas con la inscripción en Anses para recibir el IFE (Ingreso Familiar de Emergencia), mediante el ofrecimiento de realizar los trámites a cambio de un 10% del pago que iban a recibir. Desde el Anses, frente a estas maniobras fraudulentas, salieron a realizar operativos en los barrios para la inscripción de los vecinos.

Por otro lado, cuando el Gobierno Nacional lanzó la inscripción del Registro Nacional de Trabajadores y Trabajadoras, las estafas volvieron a surgir mediante la modalidad que consistía en ingresar a una página e inscribirse con la posibilidad de beneficiarse con una ayuda de 16.000 pesos, cobrando los estafadores una suma de 3.000 pesos para la inscripción[34].

Otro método comúnmente utilizado es el famoso "cuento del tío" o ingeniería social mediante el cual accedieron al home banking de dos jubiladas para sacar prestamos con altas tasas de intereses y vaciar las cuentas del Banco Provincia. Consiste básicamente en manipular o influir a la persona mediante engaño para que revelaran los datos personales de sus cuentas. Por una lado, Viviana Díaz la llamaron por teléfono diciendo que era personal de Anses para ofrecerle el IFE mediante el intercambio de número de cuenta y clave, llevándose la sorpresa de que habían pedido un préstamo por el monto de $447.000 mediante un sistema en el cual el monto final se triplica. Por otro lado, Marcela Lesniowski cayó en la estafa a través de una página de internet al solicitar un turno en el banco para retirar dólares de su cuenta para pagar una operación a fin de mes solicitándole que gestione unas claves y pasándoselas, en lo que terminaría en un préstamo por el monto de 920 mil pesos y la caja de ahorros en pesos y dólares vacía[35].

En la causa "PEDERNERA JUAN ALBERTO C/ BANCO DE LA PROVINCIA DE BUENOS AIRES S/ ACCION DECLARATIVA" el Juzgado Civil y Comercial N°10 de La Plata dictó una medida cautelar ordenando al Banco Provincia a suspender la retención de las cuotas de dos préstamos que habían sido obtenidos mediante phishing. El demandante relató que recibió una llamada telefónica en agosto del 2020 de un programa de sorteos organizado por la Petrolera SHELL comunicándole que había resultado beneficiario de la suma de $250.000. Frente a la falta de tarjeta propia para el depósito del dinero varios familiares accedieron a intervenir en terminales de pago con sus tarjetas para evitar la pérdida del premio. Posteriormente se operó desde un cajero del mismo banco vaciando las cuentas y realizando préstamos por los montos de $500.000 y $41.600[36].

[34] https://www.cibercrimen.org.ar/2020/09/20/en-aislamiento-se-multiplicaron-las-estafas-telefonicas-y-virtuales/
[35] https://www.filo.news/actualidad/Ciberdelito-Estafa-millonaria-a-dos-jubiladas-20200806-0056.html
[36] https://www.diariojudicial.com/public/documentos/000/092/576/000092576.pdf

Desde la Dirección Nacional de Ciberseguridad para evitar caer en el phishing aconsejan no abrir correos que no esperabas recibir, mirar la dirección de mail y chequear cada letra para ver si es la que figura en la página oficial del banco u organización, la misma debe contener el URL de los sitios webs (la dirección de la ubicación de las páginas). No abrir links de mensajes mal redactados, con faltas de ortográfica o sintácticas y no descargar sus archivos.

No revelar claves bancarias o personales, ninguna institución las pide por teléfono, mails, red social ni a través de empleados que vaya a domicilio. Si la contraseña entregada en el fraude es utilizada en otras aplicaciones y/o servicios es importante cambiarla rápido ya que es posible que intente probarla para obtener más datos. Si fuiste víctima de un fraude online debes realizar la denuncia en la entidad que usaron para engañarte, en la justicia o en la comisaria de tu barrio o localidad. En lo posible no borrar la evidencia, es decir, el correo recibido, enviado, los diálogos que hayas tenido y todo aquel contacto que sirva para poder resolver el caso[37].

El Ministerio Público Fiscal de CABA cuenta con una Unidad Fiscal Especializada en Delitos y contravenciones Informáticas (UFEDyCI) que concentra la investigación de delitos cometidos por medios digitales que ingresan en el ámbito de la Ciudad de Buenos Aires. Además se realizan otras funciones como capacitación de operadores del sistema judicial y brindarle las herramientas para investigar cualquier delito o contravención que se cometa por medio de internet, busca profundizar los mecanismos de Cooperación Internacional debido a que generalmente la información necesaria para el esclarecimiento de los hechos se encuentra en otros países.

Debido a la gran cantidad de denuncias, el Ministerio de Seguridad de la Nación creó un Protocolo General para la Prevención Policial del Delito con uso de Fuentes Digitales Abiertas para establecer mecanismos que las fuerzas de seguridad federal podrán disponer para detectar los delitos vinculados en internet. Esta normativa está relacionada con la emergencia pública en materia sanitaria entrando en vigencia en el Boletín Oficial mediante la resolución 144/2020.

Más recientemente la Jefatura de Gabinete de Ministros creó el Centro Nacional de Respuesta de Incidentes Informáticos (CERT.ar) con el objetivo de coordinar la gestión de incidentes a nivel nacional y prestar asistencia en el Sector Público Nacional. La disposición en el Artículo 2 dispone que las funciones serán:

a) Administrar y gestionar toda la información sobre reportes de incidentes de seguridad en las entidades y jurisdicciones del Sector Público Nacional definidas en el inciso a) del artículo 8° de la Ley Nº 24.156 y sus modificatorios.

37 https://www.argentina.gob.ar/noticias/como-evitar-el-fraude-por-suplantacion-de-identidad-en-internet-0

b) Asesorar técnicamente ante incidentes de seguridad en sistemas informáticos que reporten las entidades y jurisdicciones enumeradas en el artículo 1° de la presente medida.

c) Coordinar las acciones a seguir, ante incidentes de seguridad, con otros Programas y equipos de respuesta a incidentes de la REPÚBLICA ARGENTINA.

d) Contribuir a incrementar la capacidad de prevención, alerta, detección y recuperación ante incidentes de seguridad informática que puedan afectar activos de información críticos del país.

e) Interactuar y cooperar con equipos de similar naturaleza de otros países.

f) Llevar un registro de estadísticas y establecer métricas a nivel nacional.

g) Coordinar la gestión de incidentes de seguridad informáticos que afecten recursos críticos a nivel nacional

h) Impulsar la formación de capacidades de prevención, detección, alerta y recuperación para la respuesta ante incidentes de seguridad informática.

i) Cooperar con los gobiernos provinciales y de la Ciudad Autónoma de Buenos Aires en la gestión de incidentes de seguridad informática[38].

[38] https://www.boletinoficial.gob.ar/detalleAviso/primera/241077/20210222

Conclusión

La proliferación de los ciberdelitos provoca que la sociedad se vuelva más escéptica a la hora de la utilización de las tecnologías, las que pueden ser de gran beneficio para la comunidad. Internet influye de manera significativa en la vida de las personas y en la actividad criminal, generando nuevos medios de comisión de delitos y sirviéndose como instrumentos para la comisión de delitos transnacionales, es por ello que esta temática exige conocer las características básicas de internet. Es necesario dar a conocer los diversos tipos penales, características y los problemas que conlleva el uso de las nuevas tecnologías.

El progreso de la informática es una de las características principales de nuestra era donde resulta importantes delimitar sus usos con el fin de combatir los excesos y evitar situaciones que generen perjuicios y a su vez queden impunes. La falta de cultura informática impide parte de la lucha contra la criminalidad, por lo que resulta menester el componente educacional para la minimización de esta problemática.

Las dificultades técnicas y jurídicas que se plantean es cuestión de ciberseguridad son de orden mundial y de amplio alcance. Se deben establecer los riesgos reales y significativos de ciberseguridad insuficiente y la proliferación de los delitos.

A partir del Decreto presidencial que determino el aislamiento social y obligatorio se generaron cambios para las empresas, comercios y profesionales no esenciales en todas nuestras actividades, en el uso y el relacionamiento con la tecnología como la implementación del teletrabajo, clases a distancia o hábitos de consumo. Muchos de estos cambios llegaron para quedarse ya que encontraron una formas mas dinámica de maximizar el tiempo, de tal forma que todo esto produjo un fuerte impacto en la ciberseguridad, generando nuevos desafíos en donde buscamos protegernos de los ataques intentando acelerar los tiempos de acción.

Si bien Ley de Delitos Informáticos significó un gran avance en la materia adecuándose a la necesidad social, aún queda mucho trabajo por delante. La escasa regulación de los medios tecnológicos, se pueden observar distintas realidades por ejemplo las víctimas de estos delitos en la Ciudad Autónoma de Buenos Aires pueden denunciar los delitos en la División de Delitos Tecnológicos de la Policía Federal de Argentina ante el Área Especial de Investigaciones de Telemáticos de la Policía Metropolitana de la Ciudad Autónoma de Buenos Aires, instituciones que no existen en la mayoria de las provincias.

Diferentes provincias han reformado las leyes procesales en los últimos años dejando de lado las normas legales procesales que reglamenten el problema de la evidencia digital y la incorporación de los medios tecnológicos a efectos de dotarlos de certeza, autenticidad y valor

probatorio durante los procesos judiciales. Si bien existen distinto protocolos, reglas y pautas de buenas prácticas que sirven como guía de una investigación no resultan obligatorias en todos los casos siendo necesario suplir este vacío.

A modo de reflexión final es imprescindible intenta informar a los niños, niñas y adolescentes y sus familiares sobre cómo prevenir y evitar ser víctimas de estas conductas y concientizar las consecuencias derivadas del mal uso de las redes. Los riesgos pueden atenuarse manteniendo un protocolo de seguridad y procedimiento mediante el buen uso de las tecnologías, actualización permanentes de antivirus, etc.

Con el propósito de generar confianza y concientización es menester llevar a cabo cursos, iniciativas, y capacitaciones para hacer frente a las dificultades que entraña de las TIC, en miras a la elaboración y el fomento de estrategias de ciberseguridad siendo aspectos fundamentales para la lucha contra el cibercrimen. Resultaría conveniente la creación de fiscalías especializadas en investigación, especialmente en el interior del país, facilitaría el impulso de las causas mejorando la persecución penal en las investigaciones con presencial de personal especializado y capacitado. En otras palabras, es esencial el desarrollo de una legislación adecuada puesto que las medidas técnicas y de prevención por sí solas no pueden evitar ningún delito si el sistema no es eficiente.

Bibliografía

Acuario Del Pino Santiago (2016). Delitos Informáticos: Generalidades. Recuperado de: https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Alagia Alejandro, De luca Javier, Slokar Alejandro (2014). Revista Derecho Penal. Año III N°7. Editorial Ministerio de Justicia y Derechos Humanos de la Nación. Recuperado de: http://www.saij.gob.ar/documentDisplay.jsp?guid=123456789-0abc-defg6400-00vrsatsiver

Balmaceda Hoyos Marcelo (2011). El delito de estafa informática en el derecho europeo continental. Revista de Derecho y Ciencias Penales N°17 (111- 149) Universidad San Sebastián, Chile. Recuperado de: https://dialnet.unirioja.es/

Borzi Cirilli Federico A (2018). Suplementos Especial: Cibercrimen y delitos informáticos- Cibercrimen y evidencia digital: problemática probatoria. Editorial: Erriur.

Ciberdelitos Guía- Poder Judicial de la Provincia de Salta. Recuperado de: https://www.justiciasalta.gov.ar/es/guia-ciberdelito

Convenio sobre Ciberdelito del Consejo de Europa. Recuperado de: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

De Luca Javier A., De Rocha Joaquín Pedro (2014). Informática y delito : Reunión preparatoria del XIX Congreso Internacional de la Asociación Internacional de Derecho Penal -AIDP 1ra. edición. Ciudad Autónoma de Buenos Aires. Editorial: Infojus. Recuperado de: www.infojus.gob.ar

Delbono Patricia M (2018) Suplementos Especial: Cibercrimen y delitos informáticos- Investigación forense sobre medios digitales. Editorial: Erriur

Falbo María del Carmen (2009). Revista del Ministerio Público. Año 6 N°10. Recuperado de: https://www.mpba.gov.ar/revista.html

Gercke Marco (2014). Comprensión del Ciberdelito: Fenómenos, dificultades y respuesta jurídica. Recuperado de: www.itu.int/ITU-D/cyb/cybersecurity/legislation.html

Gómez Perals Miguel (1994). Los delitos informáticos en el Derecho Español. Ejemplar dedicado a: III Congreso Iberoamericano de informática y Derecho . Recuperado de: https://dialnet.unirioja.es/

Jean Pierre Matus A. (2017). El cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad virtual. Recuperado de: https://dialnet.unirioja.es/

Ley de Delitos Informáticos Nro. 26.388 (2008). Recuperado de: http://servicios.infoleg.gob.ar/infolegInternet/anexos/140000-144999/141790/norma.htm

Lucero Pablo. G, Kohen Alejandro A (2015). Delitos Informáticos. Bueno Aires, Argentina. Editorial: Albrematica

Parada Ricardo Antonio, Errecaborde José Daniel (2018). Cibercrimen y delitos informáticos. Los nuevos tipos penales en la era de internet. Buenos Aires, Argentina Editorial: Errelus.

Presman Gustavo (2017). Estado de la Investigación Forense Informática en Argentina para la Asociación por los Derechos Civiles. Recuperado de: https://www.errepar.com/resources/descargacontenido/CIBERCRIMEN.PDF

Sergi Natalia (2018). Análisis jurídico de la situación de la evidencia digital en el proceso penal en Argentina. Informe realizado para la Asociación por los Derechos Civiles (ADC).

Tellez Valdés Julio (2008). Derecho informático cuarta edición. México, D.F. Editorial: McGraw Hill. Recuperado de: https://clauditha2017.files.wordpress.com/2017/09/derecho-informatico-cuarta-edicion-julio-tc3a9llez-valdc3a9z.pdf