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

UNIVERSIDAD NACIONAL
DEL NORDESTE

DOCTORADO EN DERECHO

LOS DELITOS INFORMÁTICOS EN EL ORDENAMIENTO JURÍDICO ARGENTINO

AUTORA: María Josefina Álvarez

DIRECTOR DE TESIS: Edgardo Darío López Villagra

CO-DIRECTOR: Ramón Daniel Pizarro

Corrientes, 2024

ÍNDICE

ABREVIATURAS

OCDE: Organización de Cooperación y Desarrollo Económico

TIC: Tecnologías de la Información y Comunicación

TCP: Transmission Control Protocol (Protocolo de Transmisión de Internet)

IP: Internet Protocol (Protocolo de Internet)

REMJA: Ministros de Justicia o Ministros o Procuradores Generales de las Américas

INTERPOL: Organización Internacional de Policía Criminal

APEC: Foro de Cooperación Económica del Pacífico Asiático

CICTE: Comisión Interamericana contra el Terrorismo

CITEL: Comisión Interamericana de Telecomunicaciones

CSIRT: Equipos de Respuesta a Incidentes de Seguridad en Computadoras

MISPA: Reuniones de Ministros en Materia de Seguridad Pública de las América

LOS DELITOS INFORMÁTICOS EN EL ORDENAMIENTO JURÍDICO ARGENTINO

INTRODUCCIÓN

A lo largo de la historia las sociedades evolucionaron atravesando diversas etapas caracterizadas por rasgos o particularidades especiales. En lo que respecta a la actualidad la Sociedad de la Información y del Conocimiento se encuentra contextualizada en la denominada Era de la Informática o Digital en mundo sumamente globalizado. La informática ha alcanzado una enorme influencia en la vida diaria de las personas y organizaciones sociales. Así como también la importancia que tiene en el progreso mundial y en el desarrollo económico y social de un país como parte de este proceso tecnológico (Herrera Ávila, 2010). Las tecnologías de la información y la comunicación impactaron en los procesos productivos, en la velocidad de circulación de la información y en los flujos de capitales (Garzón Tapia y Vizuete Gallardo, 2009). En concreto el advenimiento de internet en el siglo XX y su progresiva mundialización implicó la aparición de nuevos paradigmas en materia de procesos de comunicación masiva.

Junto con el avance de la informática y su influencia en casi todas las esferas de la vida social, fueron intensificándose nuevos comportamientos ilícitos denominados delitos informáticos edificados y tipificados sobre la base de esta nueva realidad, dinámica, distinta y profundamente cambiante(Acosta Semblantes, 2012).

El avance vertiginoso de la computación, la informática y el uso de internet también desencadenó nuevas formas de ciberdelincuencia. Cabe señalar que el abordaje teórico-doctrinario de los delitos informáticos resulta difícil en tanto es un fenómeno sumamente complejo. El derecho tuvo que readecuar sus instituciones a los fines de conocer, describir y regular tales conductas disvaliosas. Esto explica que, sobre todo en las últimas cuatro décadas,

los Estados hayan emprendido la imperiosa tarea de establecer un marco legal estrechamente vinculado a la informática y las nuevas tecnologías. Para ello dedicaron esfuerzos para que se puedan materializar a través de herramientas jurídicas que permitan reglamentar aquellas conductas ilícitas y penalmente reprochables en el ámbito digital (González Hurtado, 2013).

Es importante anticipar que la forma en que se cometen los delitos informáticos reviste de ciertas características particulares que efectivamente los distinguen de otros delitos: acceso y alcance prácticamente ilimitados, instantaneidad, transnacionalidad, anonimato y cambios constantes, entre otros. Además, hacen que su investigación por parte de la policía y los tribunales sea mucho más compleja que en otros casos. Existen, además, diversas posibilidades para cometer este tipo de delitos facilitados por los medios, como por ejemplo amenazas, invasión de la intimidad, revelación de secretos, prostitución, corrupción de menores, exhibicionismo, etc. que potencian la importancia de un tratamiento jurídico serio y multidisciplinario de esta realidad dinámica, cambiante y, en muchos aspectos, incontrolable e impredecible. Conclusión que se potencia si se tiene en cuenta que los ilícitos informáticos pueden atentar directamente sobre la integridad de las personas como afectar a sus bienes o patrimonios (Temperini, 2018). Y más aún, contra intereses colectivos y difusos nacionales y transnacionales.

La combinación de tales características del fenómeno delictivo informático hace que sea extremadamente difícil para los legisladores y autoridades judiciales responder adecuadamente. Resulta, por ende, necesario el establecimiento de instrumentos efectivos de cooperación y coordinación internacionales para asegurar investigaciones efectivas, rápidas y coordinadas. Lo mismo se impone para el tratamiento y la preservación de evidencia digital, que en la actualidad luce frágil y volátil. Por lo que la aprobación de nuevas legislaciones específicas por parte de los Estado demanda la inmediata y eficaz adaptación a los retos que

plantean constantemente las nuevas tecnologías y la sociedad de la información (Roibón, 2008).

Desde la perspectiva de estos nuevos paradigmas, la presente investigación examinará el estudio conceptual de los delitos informáticos, así como los debates teóricos-doctrinales que se erigen en torno al fenómeno y el bien jurídico protegido en los delitos informáticos. A su vez se analizará el cibercrimen, la relación y evolución del derecho, informática y nuevas tecnologías. También se considerarán las herramientas para la efectiva investigación en entornos digitales ante la complejidad de la investigación criminal de ilícitos donde intervienen dispositivos informáticos. Se expondrán también los antecedentes y avances actuales en la legislación internacional que abordan los delitos informáticos. En este margen del derecho comparado, se desarrollará la evolución interna en la materia en el orden nacional. De este modo se analizarán las características y problemáticas que representan las normas que regulan los delitos cometidos a través de medios digitales en Argentina. Al respecto se destacará la importancia que ha tenido la Ley N° 26388 que se aprobó en el año 2008 que introduce nuevos tipos penales vinculados al uso de la tecnología en el Código Penal de la Nación.

Justificación y relevancia de la temática

En definitiva, la irrupción de las tecnologías de la información y comunicación, y en particular su utilización mediante la infraestructura de redes de internet, generó un nuevo espacio de relaciones humanas. Así, la informática revolucionó paulatinamente los sistemas jurídicos punitivos de los Estados, cimentados bajo una lógica material e ideal analógica. En efecto la utilización de dispositivos electrónicos e internet como medio de comunicación y plataforma de intercambio de bienes y servicios también devino en el surgimiento de conductas disvaliosas.

En este marco el tratamiento de los delitos informáticos se intensificó desde fines del siglo XX en los sectores doctrinarios de todo el mundo. No obstante, en Argentina aparece como un derecho de interés relativamente reciente. En efecto, la legislación penal receptó la ciberdelincuencia mediante la Ley 26388 del año 2008. En dicha normativa se configuran nuevas modalidades delictivas desconocidas para la legislación penal decimonónica y del siglo XX. Asimismo, se agregan o acondicionan algunas de las formas tradicionales delictivas a la modalidad de comisión mediante el uso de medios o herramientas propias de los sistemas informáticos. De este modo, en el ordenamiento jurídico se viene suscitando una ingente discusión en torno a los tipos existentes para regir los nuevos ilícitos que tienen lugar con el uso y abuso de los sistemas informáticos. Por lo cual es fácil advertir lo imperioso que resulta abordar a los delitos informáticos en tanto transgrede bienes jurídicos que el derecho debe proteger. De igual manera cabe señalar la necesidad de estudiar la temática debido a las problemáticas que implica su investigación y los procesos judiciales, que demandan soluciones a la legislación actual.

Una de las mayores dificultades que presentan los delitos informáticos radica en las dificultades que muchas veces encierran los aspectos probatorios y jurisdiccionales en la comprobación del hecho punible (Huerta Miranda y Líbano Manzur, 1996). Por tal motivo es relevante el tratamiento de la temática en cuanto a cuestiones referidas al valor de la prueba digital y a la jurisdicción competente para dilucidar la ley penal aplicable en delitos penales cometidos muchas veces mediante el uso de plataformas ubicadas en diferentes territorios estatales. Y también para dilucidar las nociones de tentativa en entornos virtuales, delimitar las nociones de autoría cuando se conoce el medio informático por el que se ha cometido el daño o fraude, pero se desconocen los causantes de la acción típica, entre otras aristas de los delitos informáticos. Justamente si todas las cuestiones señaladas se encuentran irresueltas, terminan por afectar a los sujetos pasivos de los delitos informáticos. Sobre todo, entendiendo

que si la justicia no puede actuar bajo parámetros fiables en la aplicación de la norma es el damnificado quien queda desprotegido ante una casuística judicial organizada en torno a interrogantes.

Problemática

En razón de lo dicho precedentemente se puede entender la importancia del problema de investigación que se orienta en torno a la siguiente pregunta: *¿Cuáles son los problemas procesales y probatorios en la aplicación de la responsabilidad penal de los delitos cometidos mediante sistemas informáticos en el marco legal argentino y su repercusión en la efectiva reparación y tutela jurisdiccional de los sujetos afectados?*

Objetivo general

- Analizar los problemas teóricos, procesales y probatorios en la aplicación de los delitos cometidos mediante internet y su repercusión en la efectiva reparación y tutela jurisdiccional de los sujetos afectados por la comisión de estos delitos.

Objetivos específicos

- Describir el avance teórico y doctrinario jurídico en materia de delitos informáticos, sus características y medios de comisión.
- Analizar el marco normativo internacional y regional en materia de comisión de delitos informáticos en cuanto a sus características y medios de comisión.
- Analizar la legislación argentina sobre delitos informáticos e identificar las dificultades de la persecución penal de los delitos cometidos mediante sistemas informáticos.

Hipótesis

La legislación penal de la República Argentina sobre delitos informáticos resulta en la hora actual insuficiente para una clara determinación de los elementos procesales y probatorios, para la calificación, persecución y pena de los delitos cometidos por medios informáticos. La persecución penal eficaz se dificulta en términos de la falta de legislación específica, la dificultad de identificación del responsable de estas conductas y los medios probatorios. Además, la evolución de las tecnologías y el surgimiento de nuevas prácticas digitales avanza más rápidamente que la adaptación de la legislación que contemple los delitos en la materia.

Marco teórico

En Argentina la Ley 26388 del año 2008 añade en el título VI de los delitos contra la propiedad dos transgresiones cometidas por medios informáticos. De esta forma se incorporó en el artículo 173 inciso 16 un caso especial de defraudación a la conducta del: "Que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos." Luego, como segundo párrafo del artículo 183, la Ley 26388 somete a la misma pena del delito de daños a la conducta del: "Que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños."

Por su parte, la Ley 25930 del año 2004 había discurrido también como un caso especial de defraudación a la acción del: "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." También en el caso de este último delito se encuentra en relación con el artículo 153 incorporado con la Ley 26388

que regula el hacking o delito de acceso no autorizado. Precisamente reprime tal conducta con prisión de quince (15) días a seis (6) meses si no resultare un delito más severamente penado al que: "A sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido".

En este marco, es el derecho procesal penal el que debe regular las garantías en perspectiva de resguardar los derechos fundamentales de los ciudadanos. En esta línea, se puede destacar que BINDER (1999) en *Introducción al Derecho Procesal Penal* define esta rama del derecho como aquella que regula en forma conjunta el poder punitivo del Estado. En términos generales, el autor refiere a la política criminal como un sistema de decisiones del Estado que, en procura de determinados objetivos, establece los delitos y las penas. Al respecto, se puede agregar que el derecho penal precisará en abstracto tanto las conductas que son punibles como las penas ante su comisión. Más aún, el derecho procesal establecerá las condiciones para que la pena pueda aplicarse en un caso concreto como puede verse en CAFFERATA NORES (2004), *Manual de Derecho Procesal Penal* y en CLARIÁ OLMEDO (2008), *El derecho procesal penal. Tomo I.* Todavía cabe señalar otras obras en la materia de autoría de LEVENE (1978), *Manual de Derecho Penal. Tomo I* de Alfredo (1968). *Derecho Procesal Penal. Tomo I.* Además del *Derecho Procesal Penal. Tomo I. Fundamentos* de MAIER (1996) y VÁZQUEZ ROSSI (2011) con *Derecho Procesal Penal. Tomo I.*

Los derechos fundamentales se originan en la propia dignidad humana y para asegurar su cumplimiento se configuran las garantías. La protección jurídica contempla el respeto de los derechos de todas las personas en el proceso. Así, las garantías son reglamentadas por los códigos procesales, en perspectiva del orden jurídico constitucional. Al respecto KÖHN GALLARDO (2016) versa con *Principios y Garantías constitucionales en el proceso penal. Una visión desde el estado social de derecho y la dignidad humana.* Del mismo modo ARES (2013) en *Garantías constitucionales en el proceso penal. Fundamentos, finalidades y*

funciones en Procesal penal 2: garantías y principios procesales. Además, se puede nombrar los trabajos de PICO I JUNOY (1997*), Las garantías constitucionales del proceso* y de PORRO y FLORIO (2016), *Las garantías constitucionales en el Derecho Procesal.*

Resulta sustancial el paradigma garantista en tanto analiza el deber ser del derecho y el ser de los sistemas jurídicos en su conjunto, es decir, las normas y la realidad. En este orden, se puede mencionar a LUIGI FERRAJOLI (1995) que distingue aquellas divergencias erigidas en torno al modelo constitucional y el funcionamiento efectivo del sistema jurídico. El juicio entre derecho y prácticas punitivas manifiesta las dificultades en el derecho penal en perspectiva de asegurar las garantías de los derechos en un sistema jurídico.

La criminalidad informática es presentada por numerosos autores como un espacio de reflexión especial, con basamento en los novedosos medios mediante los cuales se comete la ciberdelincuencia y por las diferencias que reportan estas nuevas formas comisivas para su incorporación dentro de la teoría general de la pena. En esta línea advierten MAGLIONA Y LÓPEZ (2000) que existe una confusión terminológica y conceptual en relación a los aspectos criminales de la informática. Por tanto, se debería desentrañar las acciones, omisiones y contenido de los llamados delitos informáticos, en resguardo de la seguridad social que aporta el aparato punitivo del estado.

DAVARA RODRÍGUEZ (1990) explica que no es apropiado hablar de *delitos informáticos*, ya que esta conceptualización es solamente conveniente para identificar aquellas acciones y omisiones dolosas o imprudentes que son recogidas por la ley penal. Empero dado el desenvolvimiento comisivo se relaciona directa o indirectamente con un bien o servicio informático. Asimismo, GONZALES HERRERA (2006) advierte que cuando el bien jurídico tutelado es el patrimonio, es necesario reflexionar con detenimiento las modalidades de comisión que adquieren los delitos tradicionales cometidos mediante el uso de sistemas

informáticos. De modo que se pueda cumplir así de forma cabal con el principio de estricta legalidad que requiere la ley penal.

Otros juristas, como TIEDEMANN (1985) citado en ACURIO DEL PINO (2010) avanzan en categorizar como "criminalidad mediante computadoras" a los actos antijurídicos considerados por la ley penal vigente y realizados mediante la utilización de un equipo de procesamiento de datos. En ese orden de ideas señala que esta criminalidad se representa tanto como una amenaza a la esfera privada de los ciudadanos como a los daños patrimoniales derivados del abuso del procesamiento automatizado de datos.

Estado de la cuestión

TÉLLEZ VALDÉZ (1996), en su obra *Derecho Informático, conceptúa* al delito informático en forma típica y atípica. La primera, encierra a las conductas típicas antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin. La segunda, a las actitudes ilícitas en que se tienen a las computadoras como instrumento o fin. Otro autor de referencia teórico-doctrinario es MORALES GARCÍA (2005), quien afirma: "La necesidad de asegurar la punición de ilícitos clásicos ahora fácilmente comisibles mediante nuevas tecnologías, pero difícilmente reconducibles a la redacción clásica de los delitos, so pena de interpretaciones rayana en la analogía in malampartem" (p. 396).

Debe ponderarse muy especialmente el aporte de la Organización de las Naciones Unidas sobre la clasificación de los delitos informáticos. Se configura al delito como la manipulación de los datos de entrada, salida o sustracción de datos o la manipulación de programas o la modificación de programas preexistentes en un sistema. También define como delito informático a la alteración de documentos digitales para lo cual es menester la utilización de una computadora. Cabe mencionar que oportunamente el mencionado organismo limitaba a la computadora como único medio idóneo para cometer este tipo de delitos. Sin embargo, en

la actualidad, con el avance de la tecnología, nos ha llevado a conocer otras herramientas informáticas tanto más idóneas que una PC.

La sanción de la Ley 26388 brindó un importante aporte para llenar medianamente un vacío legal existente en el derecho argentino. Entre otras cuestiones, sanciona la divulgación por la red de pornografía infantil y la violación de la correspondencia electrónica, equiparándola a la correspondencia postal. La cuestión de fondo es que no existe una definición desde el punto de vista formal de los denominados delitos informáticos, aunque internacionalmente se han propuesto diferentes definiciones. Sin perjuicio de ello, se puede afirmar que el delito informático se configura al utilizar ilegalmente un medio electrónico con el fin de realizar actividad ilegal que encuadre en figuras tradicionales. Entonces es requisito que estas figuras (estafa, robo, hurto, fraude, falsificación, daño, sabotaje) abarquen a la informática como medio para cometer la ilegalidad.

FIGARI (2009) *Reflexiones sobre la defraudación informática ley 26.388* hace un recorrido por los antecedentes de la Ley 26388 y pone de manifiesto muchas cuestiones vinculadas al funcionamiento de la misma. Es así que diversos autores coinciden en que los delitos informáticos son hechos que se cometen mediante el uso de sistemas informáticos, no importa el soporte en que se haga presente. Por ello, afirman que se trata simplemente de delitos ya existentes. En esta vía, realiza un aporte importante en la consideración de los delitos informáticos en relación a los delitos de daños. Así como también refiere sobre las cuestiones referidas a la configuración del tipo penal de daños en la nueva norma.

Es dable señalar que autores como LUZÓN CUESTA (2019), BAJO FERNÁNDEZ (2018), MATA Y MARTÍN, (2003, 2007), y SAIN (2012) realizaron estudios comentando el tipo penal de la estafa electrónica o informática como causa de perjuicio patrimonial a un tercero. Al respecto, SORBO (2013) efectuó una pormenorizada discusión sobre los aspectos teóricos de la Ley 26388. Por su parte BARRANCO GÓMEZ ALLER et al (2018) centran el

estudio de los delitos informáticos de daños en relación al derecho empresarial. En particular DAYENOF (2001) reflexiona sobre las cuestiones teóricas de los delitos penales de estafas y otras defraudaciones. Por otro lado, PALAZZI (2016, 2000) realiza un importante análisis de la Ley 26388 y la criminalidad informática. Y, SUEIRO (2017) aporta en materia de estudios de prueba digital y derecho informático penal, desde una mirada internacional.

Para profundizar aún más este debate resultaron fundamentales los trabajos de SANCINETTI (1996), DONNA (2003) *Derecho Penal, Parte Especial*. Además, no se puede dejar de mencionar a: FILLIA et al *Análisis a la reforma en materia de criminalidad informática al Código Penal de la Nación (Ley 26.388)*; Carlos REGGIANI (2008) "*Delitos informáticos*"; BARBERO *La defraudación mediante tarjeta de compra, crédito o débito según la ley 25.930* y ALONSO SALAZAR *Delito informático (Análisis comparativo con el delito de daños y otros tipos del Código Penal costarricense)* (1999); entre muchos otros que fueron de invaluable consideración para esta investigación.

Finalmente, se debe destacar el trabajo presentado por TEMPERINI (2014) *Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado. 1ra. Parte*. En dicho estudio, se afirma que los delitos informáticos son los de mayor crecimiento en los últimos años, con una proyección cada vez más acentuada. Es decir, la posibilidad de su comisión a través de la red permite que sin mayores complicaciones un delincuente pueda desde un país, usar los servicios de un segundo país, y atacar a una o más víctimas de un tercer país interviniente.

Metodología

La investigación planteó el análisis documental, tanto de doctrina como de legislación nacional e internacional. De esta manera, las fuentes de investigación, son predominantemente bibliográficas y documentales, recurriendo a material especializado en dogmática penal con

directa referencia a los delitos informáticos, revistas especializadas de derecho, doctrina nacional e internacional y análisis de fallos jurisprudenciales sobre el objeto de estudio. En este orden, se pretendió a partir de una examinación de las problemáticas teóricas, procesales y probatorias en la aplicación de los delitos de fraudes y daños cometidos mediante internet, analizar su repercusión en la efectiva reparación y tutela jurisdiccional del patrimonio de los sujetos afectados por la comisión de estos delitos.

Para alcanzar los objetivos de esta tesis se debe mencionar la metodología de la investigación jurídica, más precisamente la hermenéutica jurídica. Esta última se encarga, como bien lo dice su denominación, de hacer hermenéutica (o interpretación) de las leyes, jurisprudencias, e incluso de las hermenéuticas elaboradas por otros jurisconsultos. Siguiendo a Zaffaroni (2002) se puede decir que *"el método jurídico es fundamentalmente de interpretación de la ley y ésta se expresa en palabras (lenguaje escrito)"* (p, 79). Respecto al método jurídico en general, debemos resaltar a la metodología práctica, que se ocupa de conocer la forma en que resuelven los jueces (o un determinado órgano administrativo) una controversia jurídica. Asimismo, esta rama de la metodología de la investigación jurídica se ocupa del razonamiento, de los criterios de argumentación y de la manera en que son capaces de interpretar las normas en el caso específico resuelto por ellos.

CAPÍTULO I

DELITOS INFORMÁTICOS. PRESUPUESTOS TEÓRICOS – DOCTRINALES

1.1. Hacia una conceptualización de delitos informáticos

No existe una única definición sobre los delitos informáticos. Se trata de una cuestión doctrinariamente polémica y opinable, que se evidencia cuando se tiene en cuenta que desde los años setenta, conforme al avance de la legislación y los presupuestos teóricos y doctrinales, se fueron esbozando diferentes aseveraciones en cuanto al alcance del término. De acuerdo al Departamento de Justicia de los Estados Unidos el delito informático es "Cualquier acto ilegal donde el conocimiento de la tecnología computacional es esencial para el éxito de su prosecución" (citado en Schjolberg, 2008, p. 3).

Por su parte la Organización de Cooperación y Desarrollo Económico (OCDE) en los años ochenta sostiene que es "Cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesamiento automático de datos y/o transmisiones de datos" (citado en Estrada Garavilla, s.f., p. 2).

En la década de los noventa se destaca muy especialmente el concepto acuñado por el Consejo de Europa "Cualquier delito penal donde las autoridades de investigación deben obtener acceso a información que ha sido procesada o transmitida por sistemas computacionales o sistemas de procesamiento electrónico de datos" (citado en Schjolberg, 2008, p. 8).

En su análisis histórico, jurídico y técnico de la evolución de la informática, Huerta Miranda y Líbano Manzur (1996) presentan una conceptualización a partir de diversos autores del ámbito de los delitos informáticos. De esta manera se refieren a todos aquellos actos u omisiones típicos ilegales e intencionales, cometidos aisladamente o en serie, contra personas físicas o jurídicas que utilizan sistemas de procesamiento de información. Además, afirman

que tales ilícitos tienen como finalidad generar un perjuicio al sujeto pasivo del delito, lesionando diferentes valores jurídicos. Así como obtener algún beneficio ilícito con su comisión, sea o no de carácter patrimonial, actúe con o sin ánimo de lucro.

En términos generales, en este ámbito delictivo se suele señalar a aquellas conductas indebidas e ilegales respecto al lugar que ocupa la tecnología para la comisión del mismo (Sain, 2018). Al respecto, Salt (1997) manifiesta que los delitos informáticos "Abarca un conjunto de conductas de distintas características que afectan bienes jurídicos diversos y que son agrupadas bajo este concepto por su relación con el ordenador" (p. 6). También se puede mencionar a Altmark y a Molina Quiroga (2012) cuando lo determinan como "Actividades delictivas realizadas con la ayuda de redes de comunicaciones y sistemas de información electrónica" (p. 285).

Son también destacables aquellas conceptualizaciones que ponen de relevancia los conocimientos tecnológicos o específicos para la comisión de los delitos informáticos. En esta línea se puede ejemplificar nuevamente con Altmark y Molina Quiroga (2012) "Conductas antijurídicas no tan ordinarias, pues suponen un mínimo de conocimientos y de acceso a la tecnología, que se realizan a partir de un sistema, utilizando a éste como un instrumento eficaz para lograr el objetivo delictivo perseguido" (p. 226). Asimismo, Téllez Valdés (2003) afirma que "Son conductas criminales de cuello blanco (white collar crime), en tanto que solo un determinado número de personas con ciertos conocimientos (en este caso técnicos) puede llegar a cometerlas" (p.8).

Díaz García (s.f.) analiza los delitos informáticos desde una triple perspectiva. En principio, en tanto fin en sí mismo cuando el dispositivo electrónico es el objeto de la ofensa para manipular o dañar la información que pudiese almacenar. En segundo lugar, en tanto un medio, es decir como herramienta del hecho ilícito. Por ejemplo, cuando el sujeto activo utiliza la computadora para facilitar la comisión de un delito común. Por último, se lo puede entender

como un objeto de prueba debido a que los dispositivos informáticos almacenan elementos probatorios incidentales de los actos delictivos.

1.2.Características de los delitos informáticos

Los delitos informáticos son ilícitos en los cuales las facilidades y posibilidades para su ejecución contrastan con las dificultades de investigación. Por lo que este hecho llevó, paulatinamente, a la cooperación entre las fuerzas de seguridad y el sector privado. Justamente, por la necesidad de mantener los datos en el tráfico de los proveedores de servicios de Internet y servidores. Por tanto, los delitos informáticos tienen gran alcance y generó reconfiguraciones de los esquemas tradicionales con los cuales se concibe el derecho penal (Palazzi, 2000).

Fernández Delpech (2014) señala cuatro circunstancias que hacen que este tipo de ilícitos penales sean de difícil represión. En primer lugar, que mayormente la legislación sobre delitos informáticos y delitos cometidos en internet no tiene una tipificación específica. En segundo término, la naturaleza transnacional de los delitos informáticos, a menudo cometidas en un país, pero con consecuencias en otro Estado. En tercer orden , la falta de consenso a nivel mundial sobre la condena de determinadas acciones. Por último, las constantes innovaciones tecnológicas que suelen desarrollarse más rápido de lo que se implementan regulaciones al respecto.

Es también destacable la caracterización de los delitos informáticos que realiza Téllez Valdés (2003). Este autor estima que son ilícitos de cuello blanco (white collar crime) reservados a personas con capacidad de cometerlos pues demandan conocimientos específicos. Son delitos generalmente sofisticados en su modo de comisión. Con relación a esto último, el autor antes citado considera que su comisión frecuentemente suele tener lugar mientras el sujeto activo se encuentra trabajando. También afirma que son acciones de oportunidad en un contexto de funciones y organizaciones del sistema tecnológico y económico.

Cabe también señalar otros rasgos distintivos de esta tipología como, por ejemplo, las graves pérdidas económicas que ocasionan a los damnificados, sean personas humanas o jurídicas. En términos de ejecución pueden ser instantáneos debido a que la comisión de los delitos informáticos puede conllevar muy poco tiempo. De igual forma pueden no requerir la presencia física del sujeto activo a lo cual se puede agregar el rasgo del anonimato. Además, la comisión de los delitos informáticos tiene relación directa con las posibilidades tecnológicas de difusión masiva.

En suma, se puede advertir que los autores coinciden en que los delitos informáticos presentan grandes dificultades para su tratamiento. Los ilícitos cometidos en el marco de las particularidades de las nuevas tecnologías devienen en una investigación penal mucho más compleja que las tradicionales. El crecimiento acelerado de los delitos informáticos demanda una urgente regulación efectiva por parte del Derecho. Así, Temperini (2008) sostiene que este tipo de ilícitos son fenómenos complejos de abordar. Y, en perspectiva de otros autores, señala que sus características principales son: delitos de cuello blanco, trasnacionales, instantáneos, masivos, anonimato, pluriofensivos e investigación compleja.

1.2.1. Delitos de cuello blanco

Sain (2018) y Téllez Valdés (2003) sostienen que los delitos informáticos son aquellos denominados de “cuello blanco”, cometidos por lo general por un elenco muy selecto de personas. Es decir, específicamente aquellas que tienen conocimientos avanzados o incluso son profesionales de la informática. Por su parte, Temperini (2008) agrega matices a estas afirmaciones que limitan los delitos informáticos a la existencia de una estrecha relación con la experticia.

Se trata de una idea que requiere de prudentes matizaciones porque la realidad demuestra que no siempre es así. Los delitos informáticos pueden ser cometidos por agentes

que no encastran en aquella tradicional concepción del delito de cuello blanco, reservada para una suerte de “elite” de delincuentes, con poder económico y social generalmente relevante. Circunscribir los delitos informáticos como delitos de cuello blanco es algo que ha quedado significativamente rezagado en el tiempo y superado por la realidad . Ello por cuanto la evolución de la informática y de la (in)seguridad en la materia generó que los conocimientos sean cada vez más accesibles y difundidos para un amplio espectro de sujetos de la más variada condición económica y social. Dicho de otro modo: no es sostenible que sea necesario que los ciberdelincuentes posean conocimientos exhaustivos sobre el funcionamiento de un sistema. Basta con que sean meros ejecutores de herramientas realizadas por terceros.

En más, dado que los delitos informáticos se cometen masivamente en el escenario transnacional, el ilícito escaló hacia la automatización. A raíz de la multiplicidad de ataques se fueron configurando herramientas que ejecutan todas las tareas de forma automatizada. Por consiguiente, existen ciberdelincuentes que pueden perpetrar estos ilícitos sin que realmente alcancen a comprender las tareas que realizan aquellas herramientas. Incluso, pueden no llegar a tener un amplio conocimiento sobre el sistema informático que infringieron.

Temperini (2008) sostiene que los delitos de cuello blanco suelen estar más asociados a los ilícitos de la vieja escuela. Esto quiere decir que a las nuevas generaciones poco les interesa el conocimiento, sino que más bien se fijan en los beneficios que pueden obtener. De hecho, esta apreciación tiene que ver con el desarrollo de la ciberdelincuencia como negocio. Sobre todo, en el caso de bandas organizadas y especializadas en cibercrimen que realizan ataques que sean redituables en términos económicos.

1.2.2. Trasnacionales

Otra característica relevante de los delitos informáticos es que pueden ser cometidos a una gran distancia. No reconocen fronteras territoriales y, muchas veces, temporales. Así, el

ciberdelincuente se puede encontrar físicamente alejado del sujeto pasivo del ilícito. Justamente, las mismas potencialidades que brinda la tecnología en materia de comunicaciones brindan las posibilidades de cometer estos crímenes a distancia. A través de la conexión por internet el delincuente puede perpetrar el delito informático estando al otro lado del mundo de la víctima.

La transnacionalidad de los delitos informáticos implica que las barreras jurisdiccionales para llevarlos a cabo no son un obstáculo. Más bien, esta característica es utilizada como un potencial por los ciberdelincuentes porque las investigaciones demandan alto nivel de complejidad. Para ilustrar mejor esta idea, se debe tener en cuenta que la transnacionalidad implica otras complicaciones que van más allá de la distancia física: las dificultades relativas al idioma, la falta de legislación interna en la materia en los países implicados, la ausencia de una efectiva cooperación internacional para la justicia, entre otros factores.

Cuando los delincuentes informáticos cometen delitos que sobrepasan sus fronteras territoriales se aprovechan de este conjunto de dimensiones para hacer que las investigaciones tengan un nivel de eficacia prácticamente nulo. La complejidad del abordaje de los delitos informáticos genera en el campo del derecho preguntas sobre la legislación aplicable. Al mismo tiempo que evidencia el claro desafío de coordinar distintos ámbitos de colaboración internacional.

1.2.3. Instantáneos

De igual forma que en la característica anterior, la instantaneidad con que pueden cometerse los delitos informáticos se relaciona con otra dimensión propia de las tecnologías. Más allá de que el ciberdelincuente dedique tiempo a la inteligencia preliminar o preparación de un ataque determinado, la comisión misma de este ilícito es instantánea.

En otras palabras, se hace referencia a que el perfeccionamiento del delito se da en el mismo momento en que el delincuente lleva adelante la acción. Por ejemplo, cuando se trata de delitos informáticos de accesos indebidos a sistemas o datos restringidos, daños informáticos, o la denegación de servicio de un sitio web por unas horas, entre otros (Temperini, 2008).

1.2.4. Masivos

Al igual que la transnacionalidad y la instantaneidad, la masividad tiene relación directa con las potencialidades de las tecnologías. Así, la posibilidad de difusión masiva de contenidos es utilizada para la comisión de delitos informáticos. Por ejemplo, el envío masivo de correos electrónicos que contienen spam con ataques de phishing masivo.[1] Otro caso puede ser el envío masivo de correos electrónicos que esconden entre sus adjuntos malware con el objetivo de infectar los equipos de las víctimas.[2] Por lo que a través de estas herramientas los ciberdelincuentes buscan, detectan e infestan sistemas vulnerables. También a víctimas que no toman precauciones de seguridad de la información necesarios.

1.2.5. Anonimato

Otra de las posibilidades que brindan las tecnologías es que las personas que las utilizan pueden ocultar su verdadera identidad. Y, particularmente en el caso de las redes, puede permanecer en el anonimato la verdadera conexión desde la cual realiza sus acciones. En este

[1] El Spam es el envío masivo e instantáneo de correos con contenido publicitario sin ser solicitados y que perjudican o interfieren con el resto de mensajes recibidos (Universidad de Jaén, 2018).
El phishing es la suplantación de identidad. Es utilizado por los ciberdelincuentes para obtener información confidencial de los usuarios de forma fraudulenta y así apropiarse de la identidad de esas personas. Con este objetivo, los ciberdelincuentes envían correos electrónicos falsos para obtener contraseñas y datos personales de las víctimas (Portal oficial del Estado argentino, 2024).

[2] El malware es un programa malicioso que busca dañar a las computadoras y dispositivos móviles. Son softwares hostiles, intrusivos o molestos que se utilizan para obtener información personal, datos de cuentas bancarias o billeteras virtuales, contraseñas e información de dispositivos informáticos, entre otros delitos informáticos (Portal oficial del Estado argentino, s.f.).

sentido, el delincuente puede implementar técnicas de anonimato para la comisión de delitos informáticos para ocultar su identidad. Por tanto, el anonimato es otra de las características de este tipo de ilícitos que tiene como consecuencia el complejo desafío al momento de intentar determinar al autor del delito.

No obstante, Temperini (2008) sostiene que ninguna tecnología ofrece total anonimato para el usuario. Desde esta perspectiva, el autor postula que es más adecuado referirse a niveles de anonimato dentro del marco técnico-jurídico. En consecuencia, de acuerdo al tipo de tecnología que utilizó el ciberdelincuente será un desafío mayor o menor para el investigador averiguar la autoría. De este modo, se puede mencionar que un delito informático cometido desde un wifi público tiene un nivel bajo de anonimato. En cambio, si se realiza desde la Deep web existe un encadenamiento de proxys anónimos que complejiza mucho más la investigación (Temperini, 2016).[3]

1.2.6. Pluriofensivos

En general, cuando se hace referencia a los perjuicios o daños de los delitos informáticos se suele mencionar las grandes pérdidas económicas ocasionadas a las víctimas. Sin embargo, no es la única consecuencia, sino que es pluriofensivo en la medida que pueden afectar la intimidad, la privacidad, el honor, la reputación y la integridad personal o el normal desarrollo sexual de los menores como en los casos de grooming.[4]

Es más, los delitos informáticos pueden generar múltiples perjuicios que pueden afectar al mismo tiempo distintos ámbitos de la víctima. En relación con ello, los casos en donde hubo robo de información pueden representar una pérdida económica según el tipo de información de que se trate. Asimismo, pueden generar una sensación de inseguridad informática que para

[3] La Deep web es un espacio virtual dentro de la red de Internet en la cual los contenidos no son indexados por los motores de búsquedas tradicionales (como puede ser Google, Yahoo o Bing, entre otros) (Temperini, 2008).
[4] El Grooming es el acoso sexual de una persona adulta a una niña, un niño o un adolescente por medio de internet (Portal oficial del Estado argentino, 2024b).

la víctima resulta más grave que los daños financieros. Entonces, se debe rescatar que también influye la subjetividad de la víctima en este tipo de ilícito.

Temperini (2008) señala que los beneficios económicos para los delincuentes no siempre son cuantiosos. Inclusive algunos de los delitos informáticos que tienen como objetivo perjudicar el patrimonio de la víctima son de poco rédito, como pueden ser las estafas electrónicas. En otras palabras, salvo excepciones puntuales, los delitos informáticos suelen provocar daños relacionados directamente con lo económico a gran escala.

1.2.7. Investigación compleja

De acuerdo a lo expuesto hasta el momento, las distintas características de los delitos informáticos evidencian la complejidad en el tratamiento de este tipo de ilícitos. De esta forma, las tecnologías utilizadas con fines delictivos tienen como consecuencia una investigación mucho más compleja que las tradicionales. En principio, demanda que las fuerzas de seguridad a cargo de dichas tareas deben estar adecuadamente formadas en la materia y tener los conocimientos técnicos suficientes para prevenir, comprender, investigar y desmantelarlas maniobras delictivas y poder llevar adelante una investigación eficaz.

La investigación de los delitos informáticos requiere una capacitación especial por parte de las fuerzas de seguridad debido a la volatilidad de la evidencia digital. Por tanto, quienes cumplen estas tareas deben estar formados adecuadamente para lograr la identificación, recolección y preservación de los medios probatorios digitales. En este orden, Temperini (2008) sostiene que existen normas internacionales que guían las buenas prácticas internacionales para la adquisición de la evidencia digital. Así como también los protocolos o guías nacionales que tienen como objetivo garantizar la cadena de custodia de todos los elementos que vayan a ser incorporados a la causa como prueba.

Al respecto de la cadena de custodia cabe decir que es el “registro cronológico y minucioso de la manipulación adecuada de los elementos, rastros e indicios hallados en el lugar del hecho, durante todo el proceso judicial” (Ministerio de Justicia y Derechos Humanos de la Nación, 2015, p. 47). De esta forma, la cadena de custodia es una secuencia o serie de recaudos para asegurar el origen, identidad e integridad de la evidencia con el objetivo de evitar que se pierda, destruya o altere (Di Iorio, 2017).

Entonces, a través de la cadena de custodia se pretende preservar la fuerza probatoria de la evidencia. Por ello, se aplica a todo acto de aseguramiento, identificación, obtención, traslado, almacenamiento, entrega, recepción, exhibición y análisis de la prueba. Al mismo tiempo, garantiza la transparencia si tiene lugar algún cambio o alteración del material probatorio. Entonces, ante la inexistencia de alteraciones o variaciones durante el proceso de la cadena de custodia permite asegurar la autenticidad de la evidencia que se utilizará como prueba dentro del proceso judicial.

En relación con la necesidad de capacitación en la investigación penal, la Asociación Internacional de Derecho Penal (2014) destaca el uso de las TIC. Por lo cual se estima la necesidad de que las fuerzas de seguridad dispongan de los medios técnicos, las capacidades y la formación especializada en el uso de las TIC. Por un lado, con el objetivo de tener herramientas que se requieren para el abordaje eficaz del cibercrimen. Y, al mismo tiempo, para que puedan obtener y manejar correctamente la evidencia electrónica.

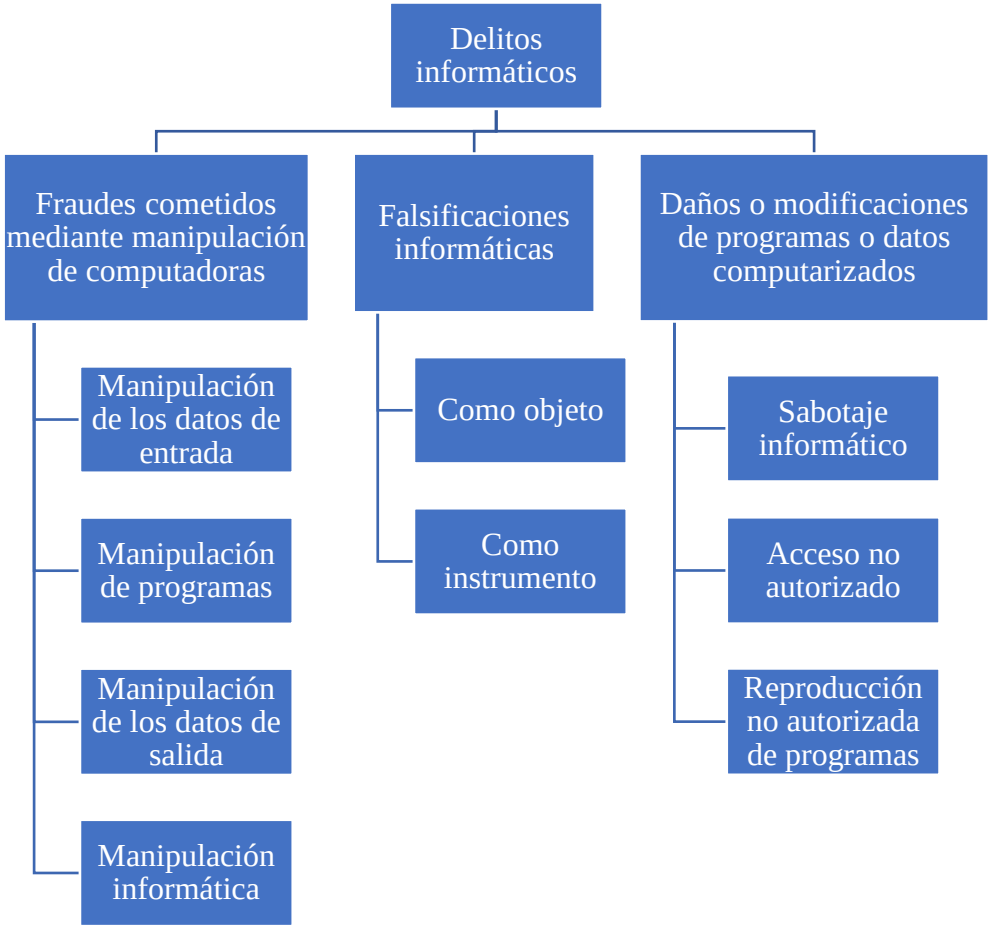
Uno de los desafíos que se presentan frente a las medidas de investigación que impliquen el uso de las TIC es la intromisión significativa en el derecho a la privacidad. Por ejemplo, con el acceso al contenido de las comunicaciones, la interceptación y el acceso de datos en tiempo real o la utilización de técnicas de investigación remota. Otro desafío sobre la investigación de delitos informáticos deviene de la necesidad de cooperación del sector privado

con las fuerzas de seguridad. Es decir, la colaboración en la investigación criminal entre las empresas privadas y/o proveedores de las TIC con las autoridades policiales.

1.3. Clasificación de la Organización de las Naciones Unidas

La Organización de las Naciones Unidas ([ONU] 1990) clasifica a los delitos informáticos en 3 tipologías: fraudes cometidos mediante manipulación de computadoras, falsificaciones informáticas y daños o modificaciones de programas o datos computarizados.

Gráfico 1. Clasificación de los delitos informáticos de la ONU



Nota. Elaboración propia en base a Vizcardo (2014)

1.3.1. Fraudes cometidos mediante manipulación de computadoras

Los fraudes cometidos mediante manipulación de computadoras dan lugar, según la clasificación de la ONU (1990) a cuatro subtipologías: manipulación de los datos de entrada, manipulación de programas, manipulación de salida y manipulación informática.

1.3.2. Manipulación de los datos de entrada

En este subtipo de fraude informático se lo suele denominar como sustracción de datos. Según Vizcardo (2014) se trata de un delito informático frecuente porque se comete con facilidad y resulta difícil de descubrir en comparación con otros ilícitos. Más concretamente porque para lograr su comisión no se requiere un amplio conocimiento técnico de informática. Por consiguiente, puede ejecutarlo cualquier individuo que tenga acceso a las funciones normales del procesamiento de datos en la fase de adquisición de ellos.

1.3.3. Manipulación de programas

Al igual que en el subtipo anterior, la manipulación de programas es muy difícil de descubrir. A menudo suele ser un delito informático que no es advertido porque para detectarlo se deben tener conocimientos técnicos muy específicos. En cuanto a su definición, la manipulación de programas consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Para ilustrar este ilícito se puede mencionar al Caballo de Troya que sirve para dar instrucciones a la computadora de modo encubierto.

A través de los troyanos el ciberdelincuente puede lograr que un programa informático pueda realizar una función no autorizada de forma oculta al mismo tiempo que su función normal. La denominación Caballo de Troya tiene el mismo sentido que en la historia griega dado que la finalidad es introducirse en el sistema como un programa inofensivo. Aunque, en

realidad, se trata de un programa que permite el control remoto de dicho sistema (Prieto Álvarez y Pan Concheiro, 2006).

1.3.4. Manipulación de los datos de salida

La manipulación de los datos de salida tiene como objetivo el funcionamiento del sistema informático para la adquisición de datos. Un ejemplo emblemático de este subtipo es el fraude mediante tarjetas bancarias robadas. Otro caso suele darse utilizando los cajeros automáticos a través de la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Conforme a la evolución de las tecnologías, para codificar la información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito se emplean equipos y programas de computadora especializados.

1.3.5. Manipulación informática

Para la comisión de la manipulación informática, el delincuente utiliza las repeticiones automáticas de los procesos de cómputo. Por tanto, es un subtipo que requiere de un conocimiento técnico especializado para su comisión. De acuerdo a Vizcardo (2014) el método más común es conocido como la "técnica salami" que se usa en las transacciones financieras. De este modo, el delincuente obtiene "rodajas muy finas" que son apenas perceptibles en dichas operaciones de dónde se sacan repetida y automáticamente de una cuenta y se transfieren a otra.

1.3.6. Falsificaciones informáticas

En cuanto a las falsificaciones informáticas, la ONU (1990) incluye dos subtipologías: como objeto y como instrumento. En el mismo sentido, Téllez Valdés (2003) clasifica a los

delitos informáticos en atención a los siguientes criterios: como instrumento o medio y como fin u objeto.

1.3.7. Como objeto

Las falsificaciones informáticas como objeto tienen lugar cuando los delincuentes alteran datos de los documentos almacenados en forma computarizada. Más precisamente, se incluyen las conductas delictivas que van dirigidas en contra de la computadora, accesorios o programas como entidad física. De esta forma, se puede tratar de la programación de instrucciones que producen un bloqueo total al sistema, la destrucción de programas por cualquier método, el daño a la memoria, o el atentado físico contra la máquina o sus accesorios.

1.3.8. Como instrumento

Las falsificaciones informáticas como instrumento refieren al uso de las computadoras como método, medio o símbolo en la comisión del ilícito. Por ejemplo, la falsificación de documentos vía computarizada (tarjetas de crédito, cheques, entre otros) y la variación de los activos y pasivos en la situación contable de las empresas. Así como también la planeación o simulación de delitos convencionales (robo, homicidio, fraude, entre otros casos). Otros ejemplos son: la sustracción o copiado de información confidencial, el aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas, la alteración en el funcionamiento de los sistemas (virus informáticos) y el acceso a áreas informatizadas en forma no autorizadas entre muchas más.

Vizcardo (2014) afirma que la creación de documentos fraudulentos de uso comercial empezó con la utilización ilícita de las fotocopiadoras computarizadas en color a base de rayos láser. En concreto, porque se convirtieron en un instrumento funcional para las falsificaciones o alteraciones fraudulentas. Justamente, porque con estas fotocopiadoras se pueden hacer

copias de alta resolución, modificar documentos e incluso crear documentos falsos sin tener que recurrir a un original. Además, los documentos que producen son de tal calidad que solo un experto puede identificar los auténticos.

Gráfico 2. Ejemplos de falsificaciones informáticas como objetivo y como medio

Como instrumento o medio	Como fin u objetivo
• Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etc.) • Variación de los activos y pasivos en la situación contable de las empresas • Planeamiento y simulación de delitos convencionales (robo, homicio, fraude, etc.) • Lectura, sustracción o copiado de información confidencial • Modificación de datos, tanto en la entrada como en la salida • Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucción inapropiadas • Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa • Uso no autorizado de programas de computo • Introducción de instrucciones que provocan "interrupciones" en la lógica interna de los programas • Alteración en el funcionamiento de los sistemas a través de virus informáticos • Accesos a áreas informatizadas en forma no autorizada • Intervención en las líneas de comunicación de datos o teleproceso	• Programación de instrucciones que producen un bloqueo total al sistema • Destrucción de programas por cualquier método • Daño a los dispositivos de almacenamiento • Atentado físico contra la máquina o sus accesorios • Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados • Secuestro de soportes magnéticos entre los que figure información valiosa con fines de chantaje

Nota. Elaboración propia en base a Estrada Garavilla (s.f.)

1.3.9. Daños o modificaciones de programas o datos computarizados

Los daños o modificaciones de programas o datos computarizados, la ONU (1990) incluye tres subtipologías: el sabotaje informático, el acceso no autorizado a servicios y sistemas informáticos y la reproducción no autorizada de programas.

1.3.10. Sabotaje informático

Es la acción no autorizada de borrar, suprimir o modificar funciones o datos de computadora con el objetivo de obstaculizar el funcionamiento normal del sistema. Una forma de comisión habitual es por medio de abusos de las fallas de seguridad de los programas que sostienen los sistemas informáticos (Martínez y Viollier, 2014). Vizcardo (2014) menciona a los virus y a las bombas lógicas como métodos usuales de sabotaje informático. Así, se debe mencionar que los virus informáticos son programas que copian o destruyen la información almacenada en un dispositivo. Las bombas lógicas "Son segmentos de código, incrustados dentro de otro programa. Su objetivo principal es destruir todos los datos del ordenador en cuanto se cumplan una serie de condiciones" (Prieto Álvarez y Pan Concheiro, 2006, p. 14).

1.3.11. Acceso no autorizado a servicios y sistemas informáticos

El acceso no autorizado a servicios y sistemas informáticos se realiza desde un lugar en el exterior situado en la red de telecomunicaciones a través de diversos medios. De esta manera, los delincuentes suelen cometer estos ilícitos aprovechando la ausencia o la baja existencia de medidas de seguridad para obtener el acceso. En este marco, una técnica utilizada es hacerse pasar por usuarios legítimos del sistema en los casos en que los usuarios emplean contraseñas comunes o de mantenimiento que están en el propio sistema.

En otras palabras, el acceso no autorizado es un ingreso sin derecho a un sistema o a una red que transgrede las medidas de seguridad. Para la ONU (2000) este ilícito es particularmente difícil de investigar porque requiere de la colaboración de la víctima y de la flagrancia del infractor. Vale señalar que algunos países tipifican el tráfico de contraseñas y prohibieron ciertos dispositivos que ayudan a la piratería informática (Martínez y Viollier, 2014).

1.3.12. Reproducción no autorizada de programas

A través de las redes de telecomunicaciones los delincuentes efectúan la reproducción de programas que no son autorizados por los propietarios legítimos. Usualmente, este subtipo de ilícito se denomina piratería informática porque se trata de una defraudación a los derechos de propiedad intelectual. Por tanto, tiene como consecuencia una pérdida económica sustancial para los propietarios legítimos (Saez Capel, 2001).

1.4.Otras clasificaciones

De acuerdo a Sans (2018), actualmente, los delitos informáticos pueden clasificarse en dos grandes grupos. Por un lado, se encuentran aquellos que demandan sofisticación técnica para su comisión. En términos generales se puede decir que esta tipología se basa en la elaboración de programas maliciosos que tienen como objetivo vulnerar dispositivos o redes. De esta forma, se cometen en lo que en informática se denomina “ingeniería técnica” porque se recurre a la elaboración de programas maliciosos.

En la segunda tipología se aglutinan los delitos informáticos relativos a amenazas, los fraudes y el grooming en donde los delincuentes actúan a través de servicios y aplicaciones web. Por tanto, muchos de ellos se cometen en lo que en informática se denomina “ingeniería social” porque el delincuente apela al proceso de la comunicación para engañar a un usuario.

Ahora bien, tanto estos delitos informáticos como los del primer grupo suelen perseguir las mismas finalidades. Sobre todo, de índole económica, como el robo de dinero. Igualmente, puede ser para la suplantación de identidad, la obtención de datos personales o institucionales de terceros.

Asimismo, se pude hacer referencia a otros tipos de delitos informáticos relacionados a la violación de la privacidad de las personas en tres niveles. Así, un nivel lo componen las intervenciones no autorizadas de los gobiernos por sobre las comunicaciones privadas de los ciudadanos. Por ejemplo, el espionaje ilegal de las agencias de inteligencia y seguridad de los Estados Unidos sobre ciudadanos extranjeros con programas de vigilancia en la lucha contra el terrorismo.

Un segundo nivel se configura en torno a la violación a la intimidad por parte de las empresas proveedoras de servicios de internet en términos comerciales. En particular, cuando actúan sin el consentimiento del usuario con el fin de conocer sus gustos y preferencias para la venta de productos y servicios asociados.

Un tercer nivel se conforma con el uso de la informática en el ámbito laboral cuando una organización empleadora accede a comunicaciones privadas de un trabajador (mails, redes sociales, etc.).

1.5.Los sujetos activos y pasivos de los delitos informáticos

De acuerdo al derecho penal se puede delimitar la existencia de dos tipos de sujetos frente a un hecho delictivo: pasivo y activo. En uno y otro polo puede haber personas humanas o jurídicas.. En este marco, la relación que se establezca respecto del bien jurídico protegido acabará por convertirse en el elemento definitorio que evidenciará el posicionamiento de los sujetos. Por consiguiente, el sujeto activo u ofensor se constituye como quien daña criminalmente el bien jurídico protegido. Por su parte, el sujeto pasivo se erige como el

propietario del bien jurídico lesionado que, a su vez, se puede diferenciar del sujeto perjudicado, que podría llegar a ser un tercero (Huerta Miranda y Líbano Manzur, 1996).

Miró Llinares (2010) sostiene que, en tanto delito común, el sujeto activo puede ser cualquier persona física o jurídica que no sea titular de los datos digitales, programas informáticos, documentos electrónicos o sistemas informáticos. Por otro lado, existen autores que prestan especial atención a los conocimientos específicos que estiman son necesarios para la comisión de los delitos informáticos. En otras palabras, que, por tratarse de un delito ligado a la tecnología, el sujeto activo requiere determinados conocimientos mínimos para que así se le pueda imputar la autoría del mismo.

El sujeto activo es considerado como persona con conocimientos informáticos. De esta forma el sujeto activo de delitos informáticos se define como aquel que intercepta en forma dolosa un sistema informático. Es decir, para apoderarse, manipular, eliminar, difundir o utilizar los datos o información digital almacenada en dispositivos tanto de organismos públicos, privados, militares, financieros como de usuarios particulares.

El sujeto activo se caracteriza por poseer conocimientos técnicos básicos que le posibilitan la comisión de delitos informáticos (Gutiérrez et. al, 2001). En esta vía Garrido (2013) delinea algunos rasgos que poseen los sujetos activos de delitos informáticos que los diferencian de delincuentes de delitos comunes:

> Los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aun cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos (p. 23).

Es dable señalar que algunos autores no dan especial importancia a que los sujetos activos de delitos informáticos posean conocimientos tecnológicos. Por ejemplo, Buompadre

(2017) afirma que el sujeto activo “Puede ser cualquier persona, sin importar el sexo ni la edad, ni el nivel de conocimiento informático que posea. Sujeto pasivo es el titular del sistema o dato informático violado” (p. 372). Entonces, se podría tratar de personas que no necesariamente sean especialistas en materia informática.

Por lo que se refiere al sujeto pasivo o víctima de los delitos informáticos. Es decir, los titulares del bien jurídico que el derecho protege y sobre la cual recae la actividad delictiva del sujeto activo del delito informático (Acurio Del Pino, 2016). Así, los sujetos pasivos son aquellos que utilizan dispositivos electrónicos, sistemas automatizados de información, programas informáticos, generalmente conectados a otros. Por tanto, en el caso de los delitos informáticos pueden ser personas físicas o jurídicas, instituciones crediticias, órganos estatales u cualquier otra organización que utilice dichos medios informáticos (Pecoy, 2012).

1.6. Conductas ilegítimas más comunes

1.6.1. Spammer

El spammer es aquel que crea y difunde mensajes no deseados, en su mayoría publicitarios. En el caso de que esta acción tenga como objetivo molestar al receptor del mensaje se puede hacer referencia al delito de acoso. Si la finalidad fuese, por ejemplo, publicitar un producto o servicio a través de estos artilugios se puede tratar de una vulneración de las normativas mercantiles, consumeriles, de lealtad comercial y de defensa de competencia. Cabe destacar que, mayormente, la ilegalidad tiene que ver con la vulneración de las leyes de protección de datos personales. Más precisamente, por la forma en la que los spammers crean sus bases de datos para la creación y distribución de estos mensajes (Cámara Arroyo, 2020).

1.6.2. Hacker

El hacker es un intruso informático (Rudi, 1994). En la jerga de la informática la palabra hacker deriva del vocablo inglés “hack” cuya traducción literal es “cortar”. Por lo que, hacker se podría traducir como “cortador” o “hachador” (Gutiérrez et. al, 2001). Desde esta perspectiva, se trata del intruso informático que intercepta ilícitamente un sistema informático que pertenece a entidades públicas o privadas, de seguridad, entidades financieras y usuarios particulares. En este tipo de incursiones las motivaciones pueden ser muy variadas, para dañar, apropiarse, interferir, desviar, difundir, y/o destruir información que se encuentra almacenada en dichos dispositivos (Villalba Díaz, 2000).

1.6.3. Cracker

El cracker también es otro intruso informático, pero el término tiene connotaciones más agresivas. Así, la terminología proviene del inglés que se traduce como "rompedor." De este modo, su definición enfatiza en que realiza acciones más nocivas que el hacker y presenta dos vertientes. Una da cuenta de que el cracker accede ilícitamente a un sistema informático y produce destrucción (borrado) o el robo de información sensible que se puede utilizar con diversos fines. La otra vertiente señala que el cracker realiza estas incursiones informáticas para desproteger todo tipo de programas, como por ejemplo transgredir las protecciones anticopia de programas comerciales.

1.6.4. Phreaker

El phreaker también es conocido como cracker telefónico porque cometen actividades ilícitas semejantes por medios distintos. Es el especialista en telefonía que utiliza las telecomunicaciones para sus actos fraudulentos. Desde esta distinción se pueden establecer las motivaciones de su acción: todo lo relacionado con el uso del teléfono o servicios telefónicos.

Usualmente, la modificación o intervención de las líneas telefónicas y las modificaciones de aparatos telefónicos con el fin de comunicarse gratuitamente (Duque Méndez y Tamayo Alzate, 2000).

1.6.5. Virucker

La denominación virucker es un término que no se utiliza en la lengua inglesa, sino que se trata de un pseudónimo que combina las palabras “hacker” o “cracker” y “virus”. De allí que la especialidad concreta de los viruckers es la creación de virus informáticos. Por ejemplo, a través de la fabricación de un programa (malware) que permite la intrusión en otros sistemas informáticos o la destrucción y alteración de datos (daños informáticos). Por consiguiente, la actividad ilícita del virucker consiste en introducir un virus informático en un sistema para destruirlo, alterarlo o inutilizarlo (Cámara Arroyo, 2020).

1.6.6. Pirata informático

El pirata informático reproduce, vende o utiliza en forma ilegítima un programa que no le pertenece o que no tiene licencia de uso, conforme a las leyes de derecho de autor. En otras palabras, es un delincuente informático que se dedica a la copia y distribución ilegal de un programa (Duque Méndez y Tamayo Alzate, 2000).

1.6.7. Espías informáticos

Al igual que los hackers y crackers, el espía informático es especialista en la intrusión informática. Sobre todo, con el objetivo de cometer robo de información, sabotaje y chantaje. En la mayor parte de los casos dirigen sus ataques contra empresas del sector privado o atentan contra los sistemas de información gubernamentales.

1.6.8. Phisher

El phisher es el que usurpa y suplanta la identidad de la víctima para la obtención de datos personales o financieros, entre otros. En general, el principal objetivo es el beneficio económico que pueda alcanzar tras recabar la información de un usuario. Para ello, el modo más habitual en que procede es el envío de correos electrónicos con algún tipo de programa espía que les permite la extracción de los datos (Cámara Arroyo, 2020).

1.7. El bien jurídico protegido de los delitos informáticos

Vale a esta altura remarcar la relevancia del debate en torno a la definición del bien jurídico protegido en los delitos informáticos. Temperini (2008) afirma que principalmente se delinean interpretaciones enmarcadas en dos corrientes doctrinarias. Por un lado, se sitúan aquellos que sostienen que los delitos informáticos no son una nueva categoría. Por otro lado, quienes afirman la existencia de un nuevo bien jurídico a proteger.

Afirman unos que los delitos informáticos simplemente son delitos tradicionales pero cometidos utilizando nuevos medios. Por consiguiente, los bienes jurídicos protegidos son los mismos de siempre. Esto quiere decir que sólo se actualizaron los tipos penales y se incorporaron nuevos medios de comisión de ilícitos comunes. En este caso se podría ejemplificar las modificaciones introducidas en los artículos 153 y 153 bis del Código Penal en la legislación argentina.

Sostienen otros que la información se erige como un nuevo bien jurídico y que requiere consecuentemente de una nueva y más enérgica forma de protección, como tal, porque tiene valor y debe ser puesto en la escena penal de forma independiente con respecto a otros bienes jurídicos. Puntualmente se debe tener en cuenta que la información puede ser interpretada como un valor de tipo económico, intrínseco de la persona, por su fluidez y tráfico jurídico, así como por los sistemas que la procesan o automatizan.

En esta línea se encuadran autores como Rovira del Canto (2002) quien señala que el delito informático es toda conducta que atenta contra el acceso y conocimiento de la información de un usuario. Por tanto, enfatiza que la información es el nuevo bien jurídico supraindividual, primordial y básico. Al respecto del carácter supraindividual refiere Hernández Díaz (2009) en relación con la confianza en el funcionamiento de los sistemas informatizados.

De este modo, cuando se alude a la idea de la seguridad informática se considera que la comisión de delitos informáticos genera daño en un doble sentido: individual y supraindividual. En concreto, transgreden bienes jurídicos individuales y concretos al mismo tiempo que pone en peligro la confianza de la sociedad en la informática. Es decir, en el buen funcionamiento de los sistemas informáticos y de las redes de transmisión de datos. Entonces, esta situación es realmente grave en pleno contexto social de dependencia respecto de las TIC para el desarrollo personal, económico y social de los individuos (Corcoy Bidasolo, 2007).

De acuerdo a Acurio Del Pino (2016) “El bien jurídico protegido, acoge a la confidencialidad, integridad, disponibilidad de la información y de los sistemas informáticos donde esta se almacena o transfiere” (p. 21). En este marco se puede mencionar la Ley N° 1273 (2009) que incorpora los delitos informáticos en el esquema penal colombiano que releva a la información como bien jurídico protegido. Asimismo, se puede ilustrar al respecto con Convenio de Cibercrimen de Budapest del año 2001 en donde se considera específicamente a los delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos.

En el marco de estos debates doctrinarios la problemática de la falta de consenso respecto del bien jurídico protegido en los delitos informáticos podría derivar en conflictos de aplicación final de los tipos penales. Es así que, desde la segunda corriente doctrinaria, se estima que la información se erige como un bien intangible, pero de claro valor en los tiempos

de la sociedad de la información. No obstante, si sigue este posicionamiento resultaría necesario puntualizar qué tipo de información se deberá proteger.

Si se comprende a la información como un nuevo bien jurídico protegido, una primera aproximación podría ser la consideración en tanto a su valor jurídico. Es decir, partiendo de los tres pilares de la seguridad de la información ya mencionados: la confidencialidad, la integridad y la disponibilidad. Es así que, dado un acceso indebido a un sistema informático, el bien jurídico afectado será la confidencialidad de la información. Sin embargo, si ocurriese un daño informático o sabotaje se conmociona la integridad. Finalmente, ante la denegación de servicios se lesionaría la disponibilidad de la información.

Temperini (2008) señala una cuestión a tener en cuenta: que los delitos informáticos se caracterizan por ser pluriofensivos debido a que "Son delitos en los cuales es posible encontrar la afectación de más de un bien jurídico a la vez" (p. 59). En consecuencia, además de la afectación de los mencionados valores jurídicos de la información, se podrían ver afectados otros tantos, como ser la intimidad de una persona, patrimonio, entre otros. Así, en esta corriente coinciden distintos autores que estiman la necesidad de protección de un nuevo bien jurídico. Los matices se erigen en torno a qué es exactamente lo que el ordenamiento debe resguardar. De este modo, Quintero Olivares (2001) sostiene que el derecho debe proteger la tecnología de internet como un nuevo bien jurídico de primera magnitud. Por su parte, Romeo Casabona (2006) señala que el ordenamiento debe ofrecer una protección jurídica más intensa a las comunicaciones personales y las actividades de producción y consumo de información en las redes.

Pese a las discrepancias doctrinales, las distintas voces de los autores en el ámbito de la delincuencia informática concuerdan en que resulta primordial la creación de una nueva categoría jurídico penal. Más precisamente, una que abarque las conductas vinculadas con el hecho informático que merece ser objeto de atención porque lesiona bienes jurídicos que

sobrepasan a los tradicionales. Por tanto, la discusión se genera porque no se arriba a la unidad de criterio para definir el bien jurídico que se pretende resguardar. En esta vía, Hernández Díaz (2009) menciona que las posturas delineadas al respecto son: la seguridad informática; integridad, confidencialidad y disponibilidad de los datos y sistemas informáticos; intimidad informática.

El posicionamiento relativo a la seguridad informática hace hincapié en que el nuevo bien jurídico a tutelar es colectivo. A su vez, estima que la protección ante las conductas que atentan contra la seguridad informática evita la lesión de una serie de bienes jurídicos de carácter individual (Carrasco Andrino, 2009). Para entender mejor esta interpretación, se debe partir de la expansión y dependencia social de las TIC del mundo actual. En consecuencia, la seguridad informática deviene en el medio idóneo para proteger los bienes a nivel individual (patrimonio, intimidad, libertad sexual, honor, etc.) y supraindividual (orden público, paz pública, seguridad del Estado) (Del Moral Tores, 2001).

Si el uso de redes y sistemas informáticos son fundamentales para el correcto funcionamiento en el ámbito público y privado, el ataque a la seguridad informática requiere de la protección de un nuevo bien jurídico colectivo. Los delitos que se cometen infringiendo la seguridad informática no sólo dañan los bienes jurídicos individuales, sino que generan riesgos para toda la comunidad de usuarios (Morillas Fernández, 2005).

Una segunda interpretación nuclea a los autores que resaltan la necesidad de proteger la integridad, confidencialidad y disponibilidad de los sistemas informáticos y de los datos contenidos en ellos. En un sentido similar a la postura anterior, tiene como base la informatización de todos los datos, tanto públicos como privados, de la sociedad actual. Ahora bien, en este caso se señala la necesidad de poder confiar en su autenticidad y en su disponibilidad plena como garantía para el desarrollo económico y social (Rodríguez Mourullo et al., 2001). Desde esta perspectiva, dicha confianza:

> Garantizaría la tutela de la incolumidad de los datos, de su libre disposición y de su mantenimiento en los términos en que los ha configurado su titular, bien jurídico también de carácter supraindividual que adelanta la intervención penal en cuanto al mismo tiempo es instrumental respecto de otros bienes jurídicos que pueden verse dañados o en peligro con el menoscabo de la accesibilidad, integridad o confidencialidad de determinados datos (Hernández Díaz, 2009, p. 238).

El tercer posicionamiento, que refiere a la intimidad informática como bien jurídico protegido, es esencialmente individual. En especial, esta postura se contempla en la doctrina italiana que entiende que ante conductas delictivas vinculadas al hecho informático el bien jurídico individual es la intimidad e inviolabilidad informáticas. Sin embargo, al igual que la vertiente anterior, se encuentra íntimamente relacionada con la seguridad informática porque reconoce que la protección debe ir encaminada a garantizar, también, la seguridad y la integridad de los sistemas informáticos (Flor, 2009).

Desde esta vertiente doctrinaria, la intimidad informática se comprende como un bien jurídico autónomo y diferenciado que requiere de protección penal específica. A partir de lo cual, el contenido central se fundamenta en el derecho del individuo a decidir acerca de la información personal que se puede o no difundir y, más aún, sobre el destino de esta posible difusión. Aunque, en base a este análisis se puede advertir que más que un nuevo bien jurídico protegido se podría tratar de una actualización de la tradicional tutela de la intimidad. En otras palabras, un derecho que garantiza la intimidad específicamente vinculada al desarrollo de la informática.

En todo caso, se debe aclarar que la protección de la intimidad informática se inscribe en perspectiva de cimentar un poder positivo de control sobre la información personal. Es decir, de la información personal a la que pueden acceder los demás individuos y el uso que pueden hacer de la misma. Desde este punto de vista, la protección de la intimidad informática se eleva

más allá del simple reconocimiento del derecho de excluir a los demás de un determinado ámbito que el titular considera reservado y que se debe proteger frente a intromisiones indeseadas. Por eso:

> Se entiende necesario este nuevo concepto, entendiendo que lo que pretende abarcar no está suficientemente garantizado ni por los tradicionales medios de tutela de la propiedad o la posesión de las cosas materiales, ni por la protección prestada al secreto, a la intimidad personal y domiciliaria o a otro tipo de bienes inmateriales (Hernández Díaz, 2009, p. 239).

1.8.Breve historia de los delitos informáticos

Con el advenimiento y la vertiginosa evolución del fenómeno informático de las TIC se produjo una revolución a escala global (Martínez, 2018). De esta manera se afirma que actualmente el mundo transita en la era de la informática "En la sociedad del siglo XXI se ha producido el tránsito de la era industrial a la de la información, nuestra economía se ha convertido en una economía de la información" (Altmark y Molina Quiroga, 2012, p. 1).

De igual forma que se generaron cambios en el desarrollo económico, las nuevas tecnologías trascienden impactando en lo político y social. En efecto se releva como una nueva forma de poder: el poder informático que posibilita el despliegue de potencialidades tanto de la sociedad como de los individuos. Sin embargo, "También se han multiplicado las posibilidades de cometer conductas disvaliosas, dañinas y peligrosas contra terceras personas, las cuales denominamos en general delitos informáticos y que en muchos casos trascienden las fronteras, alcanzando una efectiva progresión global" (Martínez, 2018, p. 34).

Sain (2018) advierte que la relación entre tecnología y delito no se inicia con el desarrollo de las computadoras e internet durante el pleno auge de la era de la informática. Ya en el siglo XIX con el telégrafo se interceptaban comunicaciones para la transmisión de

información falsa con fines económicos. A continuación, se puede mencionar lo ocurrido durante los años sesenta con la invención del teléfono, cuando se boicotea el financiamiento del gobierno al conflicto bélico de Vietnam a través del uso gratuito del servicio. Asimismo, se puede ejemplificar el pirateo telefónico realizado con cajas azules, que reproducían tonos de llamadas análogos a los de Bell Corporation y la AT&T, para establecer comunicaciones de larga distancia sin costo.

En cuanto a las computadoras Sain (2018) afirma que los primeros delitos informáticos se empiezan a manifestar en los años setenta y eran más bien de tipo económico. En esta línea el espionaje tenía como fin primordial acceder a los programas de computación, los datos de investigación en el área de defensa, la información contable de las empresas y la cartera de direcciones de clientes corporativas. En íntima vinculación al espionaje se erigía la piratería de software debido a que se trataba principalmente de la copia no autorizada de programas de computadora para su comercialización. Por su parte, el sabotaje y la extorsión informática fueron los delitos que más inquietaron a las organizaciones ante la elevada concentración de datos almacenados en formato digital.

En términos de fraude financiero, ellos tienen lugar a fines de la década del 70 y comienzos de los 80 en ocasión de que se manipularon los archivos de la base de datos empresas y los saldos bancarios para manipular las facturas de nómina. Así, entre los casos típicos se situaron la instalación de un lector de tarjetas en la entrada de los cajeros automáticos. También la instalación de un falso teclado para copiar los datos de las tarjetas de pago mediante la vulneración de la banda magnética. En este marco las empresas emisoras se vieron motivadas a adoptar medidas de seguridad relativas a la adopción de chips en los plásticos (Sieber, 1998).

En este contexto los delitos informáticos adquieren una significativa notoriedad dado al gran aumento de fraudes y al tratamiento de la problemática por parte de organismos internacionales:

> Comienza la protección normativa de los países europeos a los bienes inmateriales como el dinero electrónico, proceso iniciado por Estados Unidos en 1978. La cobertura legal de las bases de datos de las instituciones bancarias y empresas resultaba indispensable para la realización de negocios, fundamentalmente contra el robo de información comercial (Sain, 2015, p. 3).

Mientras tanto, en la década de los 90 la industria editorial, discográfica y cinematográfica se vio desbordado por la problemática de infracción a los derechos de autor. Al respecto se debe decir que la irrupción de internet propició la reproducción, intercambio y descargar en línea de obras digitalizadas, música y películas resguardadas por el copyright. Desde otra perspectiva, surgieron otras preocupaciones relacionadas a las nuevas tecnologías digitales en la red como ser la protección a la intimidad y la privacidad de las personas. También germinaron peligros vinculados a la construcción de perfiles ficticios utilizados por acosadores y pedófilos, así como la distribución de pornografía infantil (Sain, 2018).

En esta vía, muchos de los delitos informáticos mencionados hasta el momento existen desde mucho antes que existiera internet. No obstante, la inmediatez a distancia, masividad y anonimato de las nuevas tecnologías actúan como potenciadores de estafas, injurias, acoso, pedofilia, entre otros. De modo que tal combinación genera una nueva versión de los delitos y a un nuevo nivel en la forma de comisión de los mismos:

> A través de las herramientas tecnológicas, desde cualquier lugar con conexión a Internet (realización a distancia), el delincuente podrá atacar múltiples víctimas a la vez (masividad), enviando cientos de correos electrónicos a la vez, de forma instantánea (no se necesita esperar), y, de acuerdo al nivel de conocimiento del delincuente, hasta podrá

> utilizar determinados mecanismos que obstaculicen su rastreo o identificación (anonimato) (Temperini, 2018, p. 53).

Los delitos informáticos no se encuentran limitados a los ilícitos cometidos en la nube, pero si potencializan la problemática. El proceso de expansión a nivel mundial tuvo lugar con la liberalización comercial de internet a mitad de los años noventa, propiciado por el gobierno de los Estados Unidos. Fue creado para disponer de un medio de comunicación alternativo al sistema de telecomunicaciones para prevenir un hipotético colapso ante un eventual ataque nuclear soviético (Leiner et al, 2003).

Así, internet surge como red global de dispositivos electrónicos conectados entre sí, lo que permite enviar, recibir y transmitir datos e información a través del TCP/IP (Transmission Control Protocol/Internet Protocol). Por tanto, estas siglas que provienen del inglés se pueden traducir a Protocolo de Transmisión de Internet y Protocolo de Internet. En sus orígenes la conexión de red abarcaba mayormente a computadoras a diferencia de los tiempos actuales que incluye una multiplicidad de aparatos informáticos (Estrada Corona, 2004).

En consecuencia, no corresponde afirmar que los delitos informáticos son un nuevo fenómeno, al menos socialmente. Más bien cabe decir que lleva décadas de gestación, desarrollo y práctica lucrativa para los delincuentes (sujetos activos) y perjudicial para las víctimas de los mismos (sujetos pasivos). “Si bien hace años que los delitos informáticos forman parte de la delincuencia en nuestra sociedad, no deja de sorprender que en la última década el índice de ciberdelincuencia haya aumentado notoriamente” (Temperini, 2018, p. 49). Por lo que se trata de una problemática que en la era de la informática se ha hecho cada vez más visible.

1.9.Criminología del cibercrimen y ciberdelincuencia

Los términos cibercrimen y ciberdelincuencia suelen ser utilizados como sinónimos, aunque presentan algunas diferencias conceptuales. La distinción más importante se fundamenta en la organización del delito. La ciberdelincuencia se refiere a los delitos informáticos que "Ocurren a diario, tipificados penalmente, pero que ocurren de forma independiente, o individual, sin encontrar elementos o indicios que nos permitan observar organización y regularidad en la comisión de la conducta en sí" (Temperini, 2018, p. 56).

En contraste, el cibercrimen incluye aquellos delitos informáticos adquieren tinte profesional, son organizados y su comisión no se basa en motivaciones personales sino más bien económicas. En este caso, "Los sujetos pasivos de los delitos son elementos fungibles y sin interés para el ciberdelincuente, que busca optimizar sus ganancias a través del perfeccionamiento de distintas técnicas delictivas que utilizan a la tecnología como eje" (Temperini, 2018, p. 56). Por lo que existen ciberdelincuentes especializados e independientes, pero es mucho más usual que operen en bandas y con una clara distribución de tareas.

Sain (2018) analiza el cibercrimen desde un punto de vista criminológico, distinguiendo dos enfoques acerca de la naturaleza de los delitos informáticos. Por un lado, se sitúan aquellos que los comprenden como delitos tradicionales que adquieren otro matiz debido a la utilización de dispositivos informáticos y de servicios y aplicaciones en internet. Por otro lado, se encuentran los que afirman que las TIC otorgan nuevas herramientas para la comisión de delitos inexistentes, como por ejemplo la distribución de virus o programas maliciosos, ataques a sitios web y la piratería del software.

Los dos enfoques son acertados, porque los delitos convencionales revelan nuevas formas mediante el uso de dispositivos automatizados y también porque las nuevas formas delictivas se cometen a través de un programa de software o archivos digitales. En este segundo supuesto se puede ejemplificar con programas maliciosos para dañar un servidor web y afectar

el funcionamiento del sitio en línea. Al mismo tiempo, se puede mencionar los programas espías para extraer información de un dispositivo o los virus, gusanos y troyanos para alterar o dañar el funcionamiento de un dispositivo (Sain, 2012).

El cibercrimen no representa un tipo de criminalidad específica. En palabras del criminólogo Majid Yar (2006) “La delincuencia informática se refiere no tanto a un único distintivo tipo de actividad delictiva, sino más bien a una amplia gama de actividades ilegales e ilícitas que comparten en común el único medio electrónico (ciberespacio) en el que tiene lugar” (p.5). En consecuencia, el cibercrimen no se puede incluir como parte del crimen completo ni organizado.

Cabe señalar que para Sain (2018) los delitos informáticos tampoco pueden ser comprendidos como delitos de cuello blanco.

Para Sutherlard (1929 citado en Sain, 2018) el delito de cuello blanco no es cometido por delincuentes comunes sino por personas de alta estima y posición social. Tradicionalmente se afirmaba que éste nuevo fenómeno criminal podía ser cometido por un grupo reducido de personas con conocimientos especializados e incluso solamente por profesionales. Empero, actualmente, los conocimientos son cada vez más accesibles y difundidos e incluso se puede delinear la existencia de: “Una nueva generación de ciberdelincuentes que ya no poseen grandes conocimientos sobre el funcionamiento de un sistema, sino que son meros ejecutores de herramientas realizadas por terceros” (Temperini, 2018, p. 62).

De acuerdo a Sain (2018) no existe una rama o área de estudio que aborde esta problemática desde un punto de vista criminológico. Así la lucha contra los delitos informáticos y el cibercrimen presenta variados desafíos que algunas disciplinas se esfuerzan en abordar, como ser el derecho y el campo de la seguridad informática. Por su parte, Temperini (2018) sostiene que los delitos informáticos no son nuevos en términos sociales, pero “Sí podríamos aceptar que es algo “nuevo” para el derecho, y para el derecho penal en particular, al menos en

relación con el desarrollo doctrinario histórico de esta materia" (p. 49). De igual modo, Martínez (2018) sostiene que "Existe un derecho informático como rama autónoma del derecho con legislación, doctrina, jurisprudencia, formación académica y universitaria con principios propios" (pp. 32-33).

1.10. Derecho, informática y nuevas tecnologías

Tal como se mencionó en apartados anteriores con el nuevo paradigma tecnológico de las TIC se inició la transición del modelo industrial del siglo XIX hacia un nuevo modelo de desarrollo: el informacionista. "La era industrial se basó en la producción, mientras que la era de la información se fundamenta en la comunicación y la información electrónica, ambas a gran escala" (Altmark y Molina Quiroga, 2012, p. 1). Por consiguiente, la innovación tecnológica y el cambio organizativo, enfocados en la flexibilidad y la adaptabilidad, fueron condicionantes para la reestructuración del sistema capitalista (Castells, 2001).

En el modelo informacionista, la forma de organización social tiene como eje central el procesamiento y transmisión de información. Por tanto, devienen en factores primordiales de productividad y poder. En este marco la revolución de las TIC origina a nivel mundial un nuevo modo de producir, comunicar, gestionar y vivir (Castells, 2001). De esta manera la evolución del poder informático no ha sido indiferente al derecho que debe adoptar dos posturas particulares. En primer lugar, como legitimador en virtud de los magníficos beneficios que proporciona a los individuos. En segundo término , como contenedor dado los perjuicios que puede causar a las personas su utilización delictiva (Martínez, 2018).

Gradualmente se fueron creando nuevas herramientas jurídicas para buscar la protección frente a los abusos del nuevo poder informático (Martínez, 2009). En este contexto, la doctrina se tuvo que adaptar en la búsqueda de dos objetivos.. Por un lado, proteger los datos y la información digital como bienes jurídicos. Por otro lado, utilizar los dispositivos

automatizados para el mejoramiento de procesos administrativos (Sain, 2018). Tras el advenimiento de la cibernética como nueva área de estudio, el jurista estadounidense Loevigner (1949 citado en Sain, 2018) publicó Jurimetría, el próximo paso, donde analizó la aplicación de recursos informáticos para el tratamiento de la información jurídica.

En este marco se erige la informática jurídica como la primera rama disciplinar en vincular el derecho y la tecnología. En concreto, estudia la aplicación de dispositivos informáticos para el tratamiento de la información legal. Para Sain (2018) se trata de un área perteneciente al campo de las ciencias de la información y sirve al derecho para: la compilación y búsqueda de documentos jurídicos, como ayuda a los procesos jurídico-administrativos tradicionales y aquella que busca suplantar decisiones humanas mediante el uso de programas automatizados de software. Martínez (2018) hace mención al derecho informático como rama autónoma del derecho. Asimismo, Fernández Delpech (2014) conceptualiza al derecho informático como el conjunto de principios y normas que regulan los efectos jurídicos nacidos de la interrelación entre el derecho y la informática. Y que la informática es una ciencia que estudia métodos, procesos y técnicas, con el fin de almacenar, procesar y transmitir informaciones y datos en formato digital (p. 1).

Para la protección de bienes jurídicos Sain (2018) agrega que el derecho informático se encuentra dentro del campo del derecho penal. De este modo se lo define como la aplicación de las reglas jurídicas con los problemas vinculados con la tecnología. Por lo que se trata del estudio de aquellos ilícitos donde la tecnología informática reviste un papel condicionante. En el devenir histórico, los distintos bienes materiales e inmateriales fueron caratulados por los códigos penales de los países como un bien jurídico a proteger (ONU, 1994).

No obstante, la legislación penal daba preponderancia respecto de los objetos tangibles y visibles. Si bien la protección de la información y de otros objetos o valores intangibles existía ya a mediados del siglo XX, recientemente han ocurrido cambios sustanciales que le otorgaron

mayor importancia. Al respecto da cuenta el Manual sobre Prevención y Control de Delitos Informáticos (1994) que analiza las transformaciones de las últimas décadas. Así de una sociedad industrial se pasó a una sociedad posindustrial donde creció el valor de la información en los ámbitos político, económico y cultural. Por tanto, fue ganando relevancia la tecnología informática impactando en el derecho demandando nuevas respuestas jurídicas a la legislación en materia de información (ONU, 1994).

Los diferentes Estados fueron modernizando su legislación según las nuevas modalidades ilícitas denominadas delitos informáticos. En este orden se pueden delinear cuatro maneras en que abordaron la problemática en torno a la protección de la información.

Por un lado, aquellos países que tipifican convencionalmente la protección de los datos e información digital y los dispositivos informáticos. En otras palabras, se estimó como delitos contra la propiedad por ejemplo si el bien afectado era la computadora personal. Otro caso sería considerar como delitos contra la intimidad dada la intercepción del correo electrónico en tanto correspondencia personal.

En segundo lugar, están aquellas legislaciones que se reformaron e incorporaron a la información como nueva figura, es decir, como un bien jurídico a proteger. Así se puede aludir a las leyes de propiedad intelectual para la protección de los derechos de autor de obras literarias, científicas, musicales y cinematográficas. Por consiguiente, se actualizaron sus contenidos para incorporar a los programas de computación y aplicaciones de software. En última instancia se posicionan los Estados que durante los años recientes promulgaron leyes específicas sobre delitos informáticos (Sain, 2017).

En tercer lugar, está la posición de Sieber (1998) quien en un informe sobre las autoridades de la Unión Europea señala que históricamente existieron diferentes oleadas de reformas legislativas. De esta manera sostiene que el proceso de reforma comienza en los años setenta. En concreto su objetivo fue proteger la privacidad de los datos a partir de las

nuevas formas de recolección, almacenamiento y transmisión de información mediante de sistemas informáticos. En este aspecto Suecia (1973), Estados Unidos (1974) y Alemania (1977) incluyeron figuras en sus legislaciones vinculadas con la protección de los datos personales.

El jurista alemán marca una segunda oleada que inicia en el decenio de 1980. En este caso se sitúan aquellos países europeos que introdujeron la protección de los bienes intangibles frente al advenimiento de los sistemas de pago electrónico. Luego, una tercera corriente reformista se relaciona con la protección de la propiedad intelectual. Así, algunos países reformaron sus leyes de patentes en la década de 1970 para evitar la copia y venta no autorizadas de obras digitales. En esta línea se puede ejemplificar con Estados Unidos (1984), Japón (1985) y Suecia (1986) que cuentan con una legislación específica que protege obras en semiconductores y chips.

En cambio, una cuarta corriente reformista se encuentra ligada con los contenidos ilegales y nocivos, como la distribución de pornografía infantil, la incitación odio o difamación. El proceso de adaptación de las leyes tradicionales a las nuevas tecnologías se inició en Reino Unido (1994) y Alemania (1997). Es así que establecieron la responsabilidad de los proveedores de servicio y acceso a internet sobre el material publicado, en Estados Unidos (1996) y Alemania (1997). Finalmente, la última ola de reformas tuvo lugar en el campo del derecho procesal penal, en países como Australia (1971), Gran Bretaña (1984), Dinamarca (1985) y Estados Unidos (1986) (Sieber, 1998).

1.11. Investigación criminal de ilícitos en los que intervienen dispositivos informáticos

A medida que los dispositivos informáticos se integraron en la vida cotidiana de las personas la criminología tradicional tuvo que determinar nuevos tipos de peritajes. Por lo que para fines de la década de los setenta estas innovaciones se encontraban dirigidas a inscribir

nuevas formas de obtener evidencia de tipo electrónica. En esta vía en Estados Unidos desde inicios de 1980 nació como área específica la informática forense como parte del campo de la informática (Sain, 2018). De acuerdo a Noblett, Pollitt y Presley (2000) aquella es "La ciencia que se encarga de adquirir, preservar, recuperar y presentar datos que han sido procesados electrónicamente y guardados en un medio informático " (p. 1).

En cuanto a la evidencia de tipo electrónica o digital se entiende como prueba informática es “De naturaleza intangible, inmaterial, en tanto que constan de impulsos eléctricos procesados automáticamente por un dispositivo informático” (Sain, 2017, p. 8). Por tanto, consiste en datos e información almacenados, transmitidos o recibidos en equipos electrónicos. Además, tiene valor probatorio en el contexto de una investigación judicial si las circunstancias del hecho permiten sospechar la comisión de un delito.

Cabe señalar que la investigación criminal de los delitos relacionados con los dispositivos informáticos presenta algunas aristas conflictivas. Así, existen una tendencia de los delitos informáticos a la baja incidencia de denuncias judiciales a nivel mundial. Por lo que insume una amplia cifra oculta de este tipo de conductas. Al respecto Sain (2018) analiza las cifras de estadísticas criminales sobre delitos informáticos según un muestreo de denuncias judiciales en la República Argentina:

> De un total de 46.043 causas judiciales, que se tramitaron en los tribunales de todo el país en el año 2013, 221 presentaciones involucraron alguna de las figuras penales de la L. 26388 o “ley de delitos informáticos”, lo que representa un 0,48% del total. En términos del fuero criminal y correccional de la Provincia de Buenos Aires, durante ese mismo año, de 694.246 denuncias, solo 275 causas se relacionaron con dicha normativa, ocupando solo un 0,04% del total (Sain, 2018, p. 16).

Las dificultades al momento de abordar los delitos informáticos se pueden explicar por múltiples razones. Muchos de los sujetos pasivos del ilícito desconocen que son víctimas del

mismo. Asimismo, numerosos usuarios ignoran tales situaciones de agravio a la presencia de un archivo espía o spyware instalado en forma oculta en un dispositivo. Existe también el derrotero de los usuarios sobre una resolución efectiva en términos judiciales de determinados tipos de delitos. Existen, igualmente casos en torno a empresas privadas que no denuncian los crímenes informáticos por temor a afectar su imagen y reputación y/o para evitar multas o sanciones penales o administrativas.

Las dificultades para contrarrestar la criminalidad informática se relacionan con las mismas características del avance de este fenómeno. Tales cuestiones son señaladas por Davara (2002): la intangibilidad de la información como valor fundamental de la nueva sociedad y bien jurídico a proteger, las nuevas necesidades demandadas a las líneas jurídicas tradicionales y el anonimato que resguarda al delincuente informático. Así como también el desafío para obtener las evidencias digitales respecto de los delitos informáticos y las dificultades físicas, lógicas, y jurídicas del seguimiento, procesamiento y enjuiciamiento en estos hechos delictivos.

En efecto las labores de investigación judicial de delitos informáticos presentan diversos obstáculos tal como señala Lamperti (2014), “Insuficiente capacidad para compartir los datos de la investigación, dificultades técnicas para rastrear los orígenes de los ciberdelincuentes, disparidad de capacidades de investigación y capacidades forenses, escasez de personal bien preparado y una cooperación errática con otras partes responsables” (p. 1). Otro factor que dificulta la investigación de hechos delictivos informáticos es el conflicto existente en términos de jurisdicción y territorialidad. En efecto, cuando un ilícito se comete en internet puede efectuarse desde un dispositivo electrónico, pero con posibilidades de afectar a otros usuarios de cualquier lugar remoto.

De esta forma los datos digitales y la información que viajan por la red pasan por diversos enrutadores de computadoras. También se almacenan en servidores en países extranjeros, según el servicio o la aplicación web usada para distribuirlos. Por lo que, llegado

a este punto, se pueden comprender las dificultades al momento presentar una demanda en un tribunal nacional, especialmente si la empresa es una corporación multinacional. Entonces el procesamiento judicial se complica en aquellos delitos informáticos, como otros convencionales, sobre todo cuando se debe recurrir a las empresas proveedoras de servicio que almacenan registros de comunicaciones y datos de los usuarios.

En caso de solicitud del sistema judicial local, tales empresas podrán negarse a brindar información fundamentando distintos argumentos. En principio puede sostener que la solicitud se debe cursar mediante exhorto al país donde figure su sede legal debido a que no tiene representación legal en el Estado demandante. Pese a que el prestador de servicios posea representante legal en el país, su servidor está ubicado en el exterior y la solicitud debe presentarse en consecuencia con ese país. Asimismo, porque, aunque tenga una sede física y legal en el Estado y la información demandada se almacene en servidores locales, al ser una empresa del exterior se rige con la legislación de privacidad de los datos de ese país. Por tanto, no puede brindar esa información.

Cabe remarcar que la fragilidad de la evidencia digital es otro aspecto que dificulta la investigación de delitos informáticos. Pese a la existencia real de los posibles elementos probatorios, se producen en un entorno digital por lo que la escena del crimen adquiere otras características. En otras palabras, los entornos virtuales simulan representaciones de objetos físicos, por tanto, a la escena del crimen convencional que es física, se le suma el rasgo de ser lógica.

Vale tener en cuenta la flexibilidad y volatilidad de las pruebas informáticas. Se tratan de archivos que se pueden manipular o eliminar y los datos e información pueden perderse fácilmente por ejemplo ante un evento simple como la falta de suministro eléctrico, del cual depende el dispositivo electrónico. También los archivos digitales se pueden ocultar fácilmente de diversas formas: en dispositivos de almacenamiento externos, carpetas ocultas, servidores

extranjeros, almacenada en formatos especiales, dentro de otros archivos o almacenada con nombres falsos, entre otros (Sain, 2017).

Otra dificultad probatoria de las evidencias digitales es el anonimato. Resulta difícil determinar a los autores de los ilícitos en internet porque se puede ocultar la identidad real de las personas. Es así que la construcción de identidades ficticias puede ser efectuada desde sitios web y aplicaciones como ser Facebook, YouTube, WhatsApp, Twitter, Google, entre otros. Por tanto, se puede advertir la ausencia de mecanismos de acreditación de identidad certeros.

Las organizaciones criminales utilizan herramientas tecnológicas que brindan grandes niveles de anonimato. Así, recurren a espacios de intercambio en la Deep Web y realizan las operaciones ilícitas con conexiones suelen cambiar rápidamente. De esta manera, se dificulta la investigación ante la imposibilidad de localización de los delincuentes informáticos. La cooperación judicial se obstaculiza porque se conectan desde distintos proxys anónimos ubicados en diferentes lugares del mundo.

En el ámbito de los medios probatorios cabe destacar el rol de los proveedores de servicios de internet. En una investigación, la información que manejan puede ser esencial, especialmente cuando el punto de partida es una dirección IP, desde la cual se produjo una conexión. Sin embargo, estas empresas privadas no se encuentran obligadas a la conservación de ciertos datos. Por lo tanto, pueden almacenar la información o no y, sobre todo, pueden tener o no la voluntad de facilitarla a las autoridades de investigación de delitos informáticos.

> Las posibilidades de referenciar dicha dirección con una persona, depende en gran medida de la colaboración de la empresa que proveyó la misma, a fin que aporte los datos relativos al abonado como también aquellos de tráfico, o quizás de contenido, que permitan identificar al usuario o la ruta de tráfico utilizada (Cruzado, 2021, p. 39).

En consecuencia, se advierte la importancia de la preservación de la información por parte de los proveedores de servicios de internet. En función de lo cual, es necesario que exista

una regulación de los canales de comunicación entre investigador y sector privado que permitan acceder a estos datos informáticos. Asimismo, el registro y conservación de datos informáticos puede facilitar la colaboración de una investigación que transcurre en un sitio distinto de donde está erradicado la empresa proveedora. A raíz de ello, se manifiesta la necesidad de contar con mecanismos de cooperación internacional ágiles y efectivos, en razón de la volatilidad de la evidencia digital (Sain, 2012).

CAPÍTULO II

LOS DELITOS INFORMÁTICOS EN PERSPECTIVA INTERNACIONAL

2.1. Regulación en el ámbito internacional

En paralelo a la evolución de la informática se fue desarrollando en el escenario internacional cierto consenso en torno a las problemáticas del mal uso que se hace de las tecnologías. Así, los delitos informáticos se conformaron, progresivamente, en una temática de interés en el marco de los distintos organismos internacionales. De esta forma, las valoraciones político-jurídicas que se pusieron de relevancia en las reuniones de los estados miembros constituyeron, paulatinamente, la regulación internacional en la materia.

Pese a los avances que se alcanzaron a nivel internacional y las medidas adoptadas, aún persisten los problemas en la esfera de los delitos informáticos. Más allá de los esfuerzos de la cooperación internacional algunos desafíos pendientes de enfrentar son: la falta de acuerdo sobre una definición de delitos informáticos, la ausencia de enunciación jurídica de la conducta delictiva, la necesidad de formación técnica de los agentes que hacen cumplir la ley, las dificultades de carácter procesal y la falta de armonización en la legislación para las investigaciones internas en las naciones. A lo que se puede agregar la ausencia de la equiparación de los delitos informáticos en los tratados internacionales de extradición.

Teniendo presente esta situación internacional y las características de los delitos informáticos vistos en el capítulo anterior, se puede comprender que el tratamiento circunscripto a los territorios de los estados nacionales resulta insuficiente. Por consiguiente, es indispensable la cooperación internacional en el abordaje eficaz de la delincuencia informática y de las soluciones jurídicas preventivas, punitivas y resarcitorias ligadas a ella. Y, sobre todo, para que se desarrolle un régimen jurídico internacional donde se establezcan

recomendaciones de normas que garanticen su compatibilidad y aplicación adecuada (Acurio Del Pino, 2016).

Las posibilidades de comisión de los delitos informáticos se incrementan al mismo tiempo que las ventajas y las necesidades del flujo nacional e internacional de datos. Por eso cabe destacar que la criminalidad informática constituye un reto considerable para los afectados, los legisladores, los agentes encargados de las investigaciones y los funcionarios judiciales. La evolución tecnológica fue aprovechada por individuos, terroristas y organizaciones delictivas para la comisión de conductas disvaliosas. Así, la escala de esta problemática demanda que la acción no debe ser aislada. Al contrario, debe ser mediante la cooperación interinstitucional e internacional en este campo.

En cuanto a la formulación de los primeros informes y regulaciones que se refieren a la delincuencia informática a nivel internacional se debe mencionar el papel que asumieron algunos organismos como la OCDE, la ONU y el Consejo de Europa. Aunque las conclusiones y recomendaciones que fueron emitiendo carecen, en general, de poder impositivo sobre los ordenamientos de los Estados, se destaca su valor en tanto precursores. Primordialmente, como promotores de las primeras herramientas con vocación de unificar criterios a la hora de definir y clasificar a los delitos informáticos. Más aún, en el contexto de la década de 1980, en donde la dimensión internacional de la problemática comenzaba a vislumbrarse (Acurio Del Pino, 2015).

2.2. La Organización de Cooperación y Desarrollo Económico

En el marco de los esfuerzos internacionales en el abordaje de los delitos informáticos se destaca la labor de la OCDE. Es importante señalar que en 1983 comenzó a investigar la viabilidad de aplicación y armonización de leyes penales para combatir el uso indebido de los programas computacionales (Sieber, 1987). Desde la OCDE se consideró la complejidad del

crimen informático, sus posibles repercusiones económicas y su naturaleza transnacional; y se señaló el riesgo de que las distintas legislaciones internas de las naciones pudieran afectar el flujo internacional de información, entre otros.

De esta manera, desde la OCDE se realizaron intercambios de opiniones y propuestas alternativas de solución. A partir de estas deliberaciones se realizó un análisis comparativo de los derechos nacionales vigentes en perspectiva de propuestas de reforma. Las conclusiones político-jurídicas dieron lugar a una lista de conductas que los Estados podrían considerar condenables por regla general. En perspectiva de estos primeros antecedentes se destacó que el principal problema era la falta de una legislación unificada porque facilita la comisión de estos delitos.

La OCDE publicó Delitos de Informática: análisis de la normativa jurídica (1986). En este informe se reseñó las legislaciones vigentes y las propuestas de reforma en diversos Estados Miembros. Además, se incluía Lista Mínima con ejemplos del uso indebido de la informática que las naciones deberían contemplar, y así prohibir y sancionar. A su vez, gran parte de los miembros de la Comisión Política de Información, Computadoras y Comunicaciones recomendó una Lista Optativa o Facultativa para protección penal contra otros usos indebidos.

En suma, el informe de 1986 recomendó a los Estados una lista de conductas punitivas para que las incorporen a su derecho interno. Algunas de ellas fueron: el fraude y la falsificación informáticos, la alteración de datos y programas de computadora, el sabotaje y el espionaje informáticos. Otros ejemplos subrayan el acceso no autorizado, la interceptación no autorizada y la reproducción no autorizada de un programa de computadora protegido, incluido el robo de secretos comerciales (Estrada Posada y Somellera, 1998).

El informe concluyó, en consonancia con los estudios de 1983, que los delitos informáticos se caracterizan por su naturaleza transnacional. Así como también, el documento

destacó la necesidad de avanzar hacia una protección penal común en todos los Estados Miembros. En este escenario, el Consejo de Europa realizó un estudio con el objetivo de elaborar directrices en la materia. Sobre todo, en consideración del conflicto de intereses que pueden surgir entre las libertades civiles y la necesidad de protección.

En línea con las propuestas de la OCDE, el Consejo de Europa conformó un Comité Especial de Expertos sobre Delitos relacionados con el empleo de las computadoras. Así, se examinaron cuestiones relativas a: la protección de la esfera personal, las víctimas, las posibilidades de prevención, asuntos de procedimiento como la investigación y confiscación internacional de bancos de datos y la cooperación internacional en la investigación y represión del delito informático. A tales efectos, la lista mínima que sugirió la OCDE se amplió con otros tipos de abuso que fueron se estimaron sancionables penalmente.

En el desarrollo de todo este proceso de elaboración de las normas en el ámbito continental, el Consejo de Europa aprobó la resolución R(89)9 sobre delitos informáticos. En este documento se estiman aquellos casos en que los países revisen sus leyes o elaboren una nueva legislación. De este modo, se recomienda a los gobiernos de los Estados Miembros que tengan en cuenta el informe sobre la delincuencia relacionada con las computadoras y, en particular, las directrices para los legisladores nacionales (Sain, 2013).

Al respecto del trabajo que realizó el continente europeo se profundizará más adelante. Mientras tanto, en relación con la OCDE, se destaca la recomendación R(89)9 y las directrices para los legisladores nacionales. Así, los consensos a los que arribaron en el mencionado Comité Especial de Expertos también versan sobre determinados casos de uso indebido de computadoras y que deben incluirse en el derecho penal. Asimismo, elaboró una lista de actos considerados delictivos en algunos países miembros, pero que todavía carecían de un consenso internacional en favor de su tipificación.

Dentro de esta evolución legislativa es importante mencionar el trabajo que realizó la OCDE en 1992. En concreto, porque desarrolló un conjunto de normas para la seguridad de los sistemas de información con el objetivo de proporcionar un marco de referencia a los Estados y al sector privado. De esta forma, se delinearon directrices que reconocían la creciente utilización y valor de los equipos, instalaciones y redes informáticas y de comunicación. Del mismo modo que consideró que la información y los datos pueden ser almacenados, procesados, recuperados o transmitidos por estos medios.

Al igual que los precedentes de 1983 y 1986, en las directrices de 1992 la OCDE destacó la naturaleza internacional de los delitos informáticos. De la misma manera, subrayó la amplia difusión global de los sistemas de información, la importancia de su papel y la dependencia cada vez mayor en torno a ello. Especialmente, porque interviene en todos los ámbitos (económicos, sociales, culturales y políticos) y escalas (local, nacional e internacional). Así, se enfatizó en la necesidad de una mayor coordinación y cooperación internacional para enfrentar los desafíos que traía la nueva era digital

Principalmente, se señaló que, sin las debidas garantías, los datos e información en estos sistemas estaban más expuestos a ser vulnerados en comparación con los documentos físicos. En virtud de lo cual, se relevó que los sistemas de información creaban nuevos riesgos, tales como los accesos no autorizados, la apropiación indebida, alteración o destrucción. En consecuencia, se tornó evidente la necesidad de aumentar la conciencia sobre estos riesgos y explorar formas de mitigarlos dado que se carecían de medidas y procedimientos adecuados para abordar estos problemas emergentes.

Además, el informe de 1992 estableció definiciones unificadas para conceptos claves informáticos. Por ejemplo, sistemas de información, disponibilidad, integridad y confidencialidad de los datos informáticos. Igualmente, introdujo nueve principios fundamentales para combatir la delincuencia informática a nivel global: responsabilidad,

concienciación, ética, enfoque multidisciplinario, proporcionalidad, integración, velocidad, reevaluación y democrático (OCDE, 1992).

Las directrices de 1992 se actualizaron en un trabajo posterior en el año 1997 aunque con mínimas modificaciones. No obstante, experimentaron una revisión completa en el 2002, con una nueva estructura y nuevos principios de actuación. De este modo, el nuevo horizonte se construyó a partir de los nuevos desafíos surgidos con la globalización de Internet y sus implicaciones para los abusos informáticos. En esta ocasión, se mantuvieron los nueve principios mencionados, se realizaron ajustes y se agregaron tres nuevos: evaluación del riesgo, diseño y ejecución de la seguridad, y gestión de la seguridad (Alamillo Domingo, 2009).

2.3. Organización de las Naciones Unidas

En el ámbito de las organizaciones de alcance internacional, es relevante dar cuenta el trabajo de la ONU acerca del uso indebido de la informática. En principio, cabe mencionar el Octavo Congreso sobre Prevención del Delito y Justicia Penal de las Naciones Unidas que se realizó en 1990, donde se discutió la proliferación de actividades delictivas relacionadas con la informática y se analizó el hecho como una consecuencia directa de la creciente utilización de sistemas de procesamiento de información en las economías y administraciones públicas de los Estados.

En el mencionado Congreso, la intrusión transnacional en los sistemas de procesamiento de datos había captado el interés mundial. Aunque para 1990 no se habían reportado muchas modalidades de delitos informáticos, se comenzó a estimar la importancia de abordar este tipo de ilícitos. Para ese entonces, los problemas en la materia que se reiteraban eran: la reproducción y la difusión no autorizadas de programas informáticos y el uso indebido de cajeros automáticos. No obstante, se conjeturó que había un gran número de casos de delitos informáticos que no se denunciaban.

En este escenario, los países empezaron a focalizar la necesidad de establecer medidas preventivas para evitar su incremento. Justamente, se consideró que los delitos informáticos eran un fenómeno emergente y demandaba su abordaje en la comunidad internacional. Por tanto, se reconocía el potencial de consecuencias catastróficas que podrían tener lugar en este escenario con el uso indebido de la informática. En vista de lo cual, el Congreso sugirió que se sancionaran pautas y directrices sobre la seguridad de los sistemas informáticos (Estrada Posada y Somellera, 1998).

El Informe general del Octavo Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal (1990) destacó la necesidad de establecer medios de cooperación internacional en asuntos penales sobre ilícitos informáticos. En adhesión a la OCDE reconoció que los sistemas informáticos implican nuevos desafíos. Así, puntualizó en que el almacenamiento de datos sensibles de índole política, económica, médica, social y personal daban lugar a nuevas formas de delincuencia.

Entre las medidas recomendadas se incluyó: la actualización de las normas y procedimientos internos de los países, el fortalecimiento de la seguridad de los sistemas informáticos, y la implementación de iniciativas de sensibilización de la opinión pública. Igualmente, se sugirió la capacitación de funcionarios encargados de la prevención, investigación y sanción de los delitos informáticos, especialmente los jueces y los cuerpos de seguridad (González Hurtado, 2013).

Desde la ONU se apeló a los Estados miembros para que intensificaran sus esfuerzos ante este tipo emergente de criminalidad informática y se promovió el desarrollo de directrices internacionales con el objetivo de armonizar en los Estados las consecuencias legales de estos ilícitos. Además, se solicitó al Secretario General de la ONU que considerara la elaboración y publicación de un documento técnico sobre la prevención y enjuiciamiento de delitos informáticos para el periodo 1992-1993.

Es importante mencionar el trabajo de la ONU en el estipulado de lineamientos para que los Estados y el sector privado pudieran erigir un marco de seguridad que proteja los sistemas informáticos. En este orden, siguió la línea de esfuerzos realizados anteriormente por la OCDE con la elaboración del Manual de las Naciones Unidas sobre Prevención y Control de Delitos Informáticos (1994). Así, el Manual devino en una de las herramientas más importantes a nivel internacional de abordaje de los delitos informáticos.

En el Manual, la ONU señala que la problemática es realmente grave porque se eleva a la escena internacional dada su naturaleza transnacional. En consecuencia, con este carácter se magnifican los inconvenientes y las insuficiencias en tanto constituyen una nueva forma de crimen. Es por ello que, fundamentalmente su tratamiento demanda una eficaz cooperación internacional. De acuerdo a Acurio del Pino (2015), la ONU resume las dificultades en el área de los delitos informáticos de la siguiente manera:

- Falta de acuerdos globales acerca de qué tipo de conductas deben constituir delitos informáticos.
- Ausencia de acuerdos globales en la definición legal de dichas conductas delictivas.
- Falta de especialización de las policías, fiscales y otros funcionarios judiciales en el campo de los delitos informáticos.
- Ausencia de armonización entre las diferentes leyes procesales nacionales acerca de la investigación de los delitos informáticos.
- Carácter transnacional de muchos delitos cometidos mediante el uso de computadoras.
- Ausencia de tratados de extradición, de acuerdos de ayuda mutuos y de mecanismos sincronizados que permitan la puesta en vigor de la cooperación internacional.

Empero, durante el Noveno Congreso sobre Prevención del Delito y Justicia Penal (1995) no se hizo mención concreta a los delitos informáticos. Si bien el informe final destacó la relevancia de la cooperación internacional en la lucha contra diversos tipos de delitos, no se

incluyeron recomendaciones específicas sobre delitos informáticos. Este hecho resulta sorprendente dado el contexto de rápido desarrollo de los sistemas informáticos y la proliferación de Internet. Más aún, porque hacía apenas un año que se había publicado el Manual mencionado sobre la acuciante problemática.

El Informe general (1995) del Noveno Congreso no propone medidas concretas respecto del ámbito de los delitos informáticos pese a su marcado carácter transnacional. Solamente incluye a los delitos informáticos entre la enumeración exhaustiva de las distintas amenazas que plantea la delincuencia transnacional organizada.[5] Recién en el Décimo Congreso sobre Prevención del Delito y Justicia Penal vuelve a ser un tema central. Aunque, en el Informe General (2000) cambia la denominación a delitos relacionados con las redes informáticas que demuestra "la necesidad de realizar nuevas apreciaciones a las efectuadas en el 8º Congreso y en los trabajos de 1992 y el Manual de 1994" (González Hurtado, 2013, p. 65).

Junto al cambio de denominación, se destaca que el Informe General (2000) incluye un apéndice que detalla la evolución histórica de los aspectos internacionales relacionados con el tema. Y, tras destacar la proliferación de Internet como un cambio significativo, se centra en llamar la atención de los Estados miembros para la armonización de los marcos legales nacionales. Así, en amplio sentido se refiere a la legislación tanto del ámbito penal como procesal y jurisdiccional en general.

[5] Los delitos terroristas y sus vínculos, los actos de violencia en zonas urbanas, el tráfico ilícito de drogas, el tráfico ilícito de armas, el tráfico internacional de menores, el tráfico ilícito de extranjeros, los delitos económicos, la falsificación de moneda, los delitos ecológicos, la corrupción, los delitos contra el patrimonio cultural, el robo de vehículos de motor, **los delitos relacionados con la informática y las telecomunicaciones**, el blanqueo de dinero, la infiltración por grupos de delincuentes organizados de las economías legítimas (el destacado en negrita pertenece al autor).

Asimismo, el Informe General (2000) destaca otro de los caracteres de los delitos informáticos: la distancia. Más precisamente, refiere a que su comisión a través de Internet implica que los perpetradores pueden estar en lugares remotos. Tal naturaleza dificulta su localización y su posterior procesamiento judicial en los lugares donde sus acciones tuvieron efecto. En este marco, concluye haciendo hincapié en la necesidad de redoblar esfuerzos en lo sucesivo para garantizar que Internet sea un entorno seguro para el intercambio social, económico y cultural. Y, más aún, enfatiza en la importancia de una mayor colaboración internacional.

Recapitulando: tanto el Octavo como el Décimo Congreso marcaron hitos importantes en el tratamiento de la delincuencia informática por parte de la ONU. A continuación, tiene lugar un proceso de consolidación de la temática en cuanto es de tratamiento recurrente en las siguientes ediciones. Bajo diferentes nomenclaturas estuvo presente en los Congresos quinquenales de la ONU: “Seminario sobre medidas para combatir los delitos informáticos” (Décimo primer Congreso) y “Novedades recientes en el uso de la ciencia y la tecnología por los delincuentes y por las autoridades competentes en la lucha contra la delincuencia, incluido el delito cibernético” (Duodécimo Congreso).

En el Informe General del Décimo primer Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal (2005) se abordaron nuevas formas de delincuencia informática en el contexto del crecimiento de Internet. En concreto, se mencionan las prácticas de utilización de identidades falsas para obtener datos íntimos como contraseñas y cuentas bancarias de las víctimas (phishing). Así como también en la ingeniería social que se utiliza: el engaño a través de la solicitud por correo electrónico u otros medios de contacto digital o la aparición de webs fraudulentas con este fin. Es decir, que ya no se trata solamente de ingeniería técnica para su comisión, porque se realizan sin necesidad de utilizar virus u otros programas complejos (Faith Cranor, 2010).

Cabe señalar que en el Informe General (2005) se refiere a la proliferación de redes inalámbricas locales y su potencial impacto en la delincuencia informática para los años subsiguientes. Una vez más, se insistió en la importancia de la colaboración internacional en consonancia con la aprobación del Convenio sobre Ciberdelincuencia de Budapest (2001). En contraste, el siguiente Congreso (duodécimo) fue de menor contribución dado que introdujo escasas novedades.

Así, en el Informe General (2010) se destacaron nuevamente las dificultades para perseguir delitos informáticos a través de Internet. De igual modo, se enfatizó en la necesidad urgente de colaboración judicial internacional. La novedad más importante se erige en torno a que, por primera vez, se reconoció la vulnerabilidad de los países en desarrollo frente a estos delitos debido a las limitaciones técnicas en su persecución. Es por ello que se insta a los países desarrollados a proporcionar apoyo. Nuevamente, se renovó el llamado a establecer un marco internacional obligatorio para combatir la delincuencia informática. Asimismo, se propuso la creación de un nuevo convenio internacional similar al de 2001.

2.4. Convenio sobre la ciberdelincuencia de Budapest

Desde una perspectiva internacional, la aprobación del primer instrumento de carácter obligatorio sobre delitos informáticos marcó un hito en la materia. Así, los esfuerzos del Consejo de Europa dieron sus frutos en el 2001 con el Convenio sobre la Ciberdelincuencia en Budapest (Chicharro Lázaro, 2009; Sánchez Bravo, 2002). Además de los Estados miembros de la Unión Europea, participaron en la elaboración y suscribieron a dicho Convenio los Estados Unidos, Canadá, Sudáfrica y Japón.

Por tanto, es relevante advertir el alcance de la cooperación internacional en la búsqueda de armonizar las distintas legislaciones penales sobre estos ilícitos. Sin lugar a dudas, se trata del instrumento internacional más importante en relación con la ciberdelincuencia, tanto por

su contenido como por el amplio consenso alcanzado (De La Cuesta Arzamendi y De La Mata Barranco, 2010). Al respecto, la Comisión Europea (2010) afirma que el Convenio de Ciberdelincuencia es la normativa internacional más completa porque establece un marco global y coherente que abarca los diversos aspectos de esa problemática.

Cabe aclarar que las disposiciones del Convenio no son de aplicación directa. En otras palabras, la obligatoriedad viene de que su contenido debe ser entendido como una guía impuesta que los Estados deben seguir en la elaboración de sus legislaciones. De este modo, el texto del Convenio insta a los Estados adheridos, ante la necesidad de reforma en la materia, a adoptar las medidas legislativas consensuadas y aprobadas (Morillas Cueva y Cruz Blanca, 2009).

Pese a que la implementación del Convenio en la Comunidad Internacional se produce paulatinamente, no se puede negar que su vigencia es de gran valor, sobre todo por la capacidad que tiene el texto de proporcionar una base de protección adecuada. A partir de allí, los resultados materiales se medirán según el número de Estados que lo ratifiquen y apliquen (Sánchez Siscart, 2011). Una vez más, se somete a prueba la necesidad de la cooperación internacional ante un tipo de delito que traspasa las fronteras nacionales. “El carácter transfronterizo o desterritorializado de muchas de las manifestaciones de la delincuencia que utiliza sistemas informáticos nos indica que cualquier medida normativa que no sea de carácter universal contiene vías de escape” (Pérez Gil, 2004, p. 1806).

De acuerdo a Acurio Del Pino (2016) el Convenio sobre la Ciberdelincuencia tiene como objetivos fundamentales:

- Armonizar las leyes penales sustantivas aplicables a las conductas delictivas que tienen como escenario el entorno informático.

- Proveer reglas de procedimiento penal que brinden a las autoridades nacionales competentes las facultades necesarias para la investigación y persecución de tales conductas delictivas.
- Establecer un régimen dinámico y efectivo de cooperación internacional.

En el preámbulo del Convenio se enuncian los objetivos que persigue en consideración de que se trata de un trabajo que da continuidad a los precedentes esfuerzos internacionales. De este modo, el texto cita un amplio abanico de tratados internacionales y convenciones que van desde los derechos humanos hasta la cooperación en materia penal y en relación con el ámbito de la informática y las telecomunicaciones (González Hurtado, 2013).

En este orden, el preámbulo del Convenio sobre la Ciberdelincuencia refiere a su adhesión a las iniciativas de las distintas organizaciones internacionales, como ser la ONU, la OCDE, la Unión Europea y el G8. Sin embargo, por fuera del ámbito de los derechos humanos, el texto sólo menciona explícitamente las convenciones, recomendaciones y resoluciones de la comunidad europea:

- Convenio del Consejo de Europa de 1981 para la protección de las personas con respecto al tratamiento informatizado de datos personales.
- La Recomendación del Comité de Ministros R(85)10 relativa a la aplicación práctica del Convenio europeo de asistencia judicial en materia penal en relación con las comisiones rogatorias para la vigilancia de las telecomunicaciones.
- La Recomendación R(88)2 sobre medidas encaminadas a luchar contra la piratería en materia de propiedad intelectual y derechos afines.
- La Recomendación R(87)15 relativa a la regulación de la utilización de datos personales por la policía.
- La Recomendación R(95)4 sobre la protección de los datos personales en el ámbito de los servicios de telecomunicaciones, con especial referencia a los servicios telefónicos.

- La Recomendación R(89)9 sobre la delincuencia relacionada con la informática, que ofrece a los legisladores nacionales directrices para definir ciertos delitos informáticos.
- La Recomendación R(95)13 relativa a los problemas de procedimiento penal vinculados a la tecnología de información.
- La Resolución N°1 adoptada por los Ministros de Justicia europeos, en su XXI Conferencia, que recomendaba al Comité de Ministros apoyar las actividades en relación con la ciberdelincuencia organizadas por el Comité Europeo para Problemas Criminales con el fin de aproximar las legislaciones penales nacionales y permitir la utilización de medios de investigación eficaces en materia de delitos informáticos.
- La Resolución N° 3 adoptada en la XXIII Conferencia de Ministros de Justicia europeos que exhortaba a las partes negociadoras a persistir en sus esfuerzos por encontrar soluciones que permitan al mayor número posible de Estados ser partes en el Convenio, y reconocía la necesidad de disponer de un mecanismo rápido y eficaz de cooperación internacional que tenga debidamente en cuenta las exigencias específicas de la lucha contra la ciberdelincuencia.
- Plan de Acción adoptado por los Jefes de Estado y de Gobierno del Consejo de Europa, con ocasión de su Segunda Cumbre para buscar respuestas comunes ante el desarrollo de las nuevas tecnologías de la información, basadas en las normas y los valores del Consejo de Europa.

Así, en el preámbulo del Convenio sobre la Ciberdelincuencia se reconoce la "necesidad de aplicar, con carácter prioritario, una política penal común encaminada a proteger a la sociedad frente a la ciberdelincuencia, entre otras formas, mediante la adopción de la legislación adecuada y el fomento de la cooperación internacional." En este sentido, para González Hurtado (2013) se trata de algo novedoso con respecto a las anteriores regulaciones de origen internacional dada "la pretensión de conseguir una armonización en el ámbito penal

desde un punto de vista de política legislativa proveniente de un órgano de naturaleza supranacional, pero con un carácter netamente imperativo" (p. 87).

El Convenio sobre la Ciberdelincuencia se basa en el reconocimiento de la necesidad de armonización de las legislaciones nacionales en la materia. Para ser más claros, con la urgencia de disponer de una herramienta común, sustantiva y adjetiva, para lograr el procesamiento de los delitos informáticos. Así, el fin último que se propone con este elemento comunitario es mejorar la cooperación internacional entre los Estados parte. Por lo cual, se estima que la aplicación de una normativa común de carácter supranacional va a permitir a los Estados el intercambio de información y pruebas necesarias para la investigación de estos ilícitos.

Ahora bien, para que esto sea realmente efectivo y exista una verdadera cooperación y ayuda jurídica mutua resulta esencial que este tipo de convenios entre en vigor. De esta manera, se podrían unificar los tipos penales existentes sobre la delincuencia informática para alcanzar la correlación o correspondencia entre los tipos penales en las diferentes jurisdicciones nacionales. En palabras de Acurio Del Pino (2015): "de hecho, cuanto más alcance tengan las leyes, tanto menor será el número de refugios desde la delincuencia informática organizada puede operar con impunidad" (p. 47).

Nuevamente, como en otros instrumentos, el énfasis se encuentra en la necesaria armonización de las leyes sustantivas y procesales a nivel internacional. En consecuencia, el esfuerzo requiere darse en todos los países que deben revisar sus procedimientos sobre las pruebas, el registro e incautación de los efectos de este tipo delictivo. Los países deben considerar su naturaleza compleja, la globalidad de Internet y sus diferentes servicios que abarca la información digital y los sistemas modernos de computación y comunicación. Una mayor coordinación de las leyes sustantivas y procesales facilitaría la cooperación en las investigaciones que trascienden múltiples jurisdicciones.

Según Oliver Muñoz Esquivel (2002) el Convenio sobre la Ciberdelincuencia constituye el esfuerzo internacional más importante en contra de las actividades criminales cometidas a través de medios informáticos. Resulta esencial la cooperación internacional porque Internet se constituye como un vehículo adecuado para la propagación de actos criminales bajo condiciones de anonimato. En más, porque se transformó en el entorno más utilizado para la financiación de estas actividades. Por ello, corresponde a los Estados:

> La responsabilidad de reconocer la importancia de establecer sanciones y mecanismos de investigación adecuados, que sean lo suficientemente avanzados y dinámicos como para hacer frente a este tipo de actividades delincuenciales que afectan a la raíz misma de nuestra sociedad (Acurio Del Pino, 2015, p. 48).

Luego del preámbulo, el Convenio sobre la Ciberdelincuencia se desarrolla a lo largo de cuatro capítulos. Así, inicia con un primer capítulo muy breve en el que se conceptualiza una serie de terminologías específicas del ámbito que regula el Convenio. En el segundo capítulo se delinean las medidas que los Estados deben adoptar en materia de derecho penal sustantivo (sección 1), derecho procesal (sección 2) y jurisdicción sección 3). El tercer capítulo se refiere a los procedimientos de cooperación internacional en esta materia: principios generales (sección 1) y disposiciones específicas (sección 2). El cuarto y último capítulo lo componen las cláusulas finales que abarcan aspectos tales como la aprobación, formas de adhesión y firma, denuncias, enmiendas, reservas, entre otros.

Por lo que se refiere al primer capítulo, contiene varias definiciones de términos que son necesarios para comprender el espíritu del Convenio sobre la Ciberdelincuencia (2001). Se pretende el establecimiento de una terminología común para todos los Estados a los efectos del mutuo entendimiento. En concreto, se conceptualiza al sistema informático, datos informáticos, proveedor de servicios y datos relativos al tráfico (Acurio Del Pino, 2016).

- Por “sistema informático” se entiende cualquier dispositivo aislado o un conjunto de dispositivos interconectados o relacionados. Además, se define que su función, o al menos la de alguno de sus elementos, es el tratamiento automático de datos en ejecución de un programa.
- Por “datos informáticos” se comprende cualquier representación de hechos, información o conceptos que permita el tratamiento en un sistema informático. Inclusive, los programas diseñados para que un sistema informático realice una función.
- Por “proveedor de servicios” se entiende a toda entidad pública o privada que ofrece a los usuarios el servicio de comunicación mediante un sistema informático. Por otra parte, este término concibe a cualquier otra entidad que pueda procesar o almacenar datos informáticos para dicho servicio o para los usuarios del mismo.
- Por “datos relativos al tráfico” se comprende cualquier dato relativo a una comunicación realizada a través de un sistema informático, producidos por éste como elemento de una cadena de comunicación. Así como también, con la capacidad de indicar el origen, destino, ruta, hora, fecha, tamaño, duración de la comunicación o tipo de servicio subyacente.

En el segundo capítulo el Convenio sobre la Ciberdelincuencia (2001) refiere a las medidas que deben ser tomadas a nivel nacional. Así, en el texto aparecen las prácticas que se recomienda que deben ser tenidas en cuenta como conductas típicas en las legislaciones penales de los Estados adheridos (Foggetti, 2003; Rodríguez Bernal, 2007). Asimismo, este capítulo presenta una sección primera que se dedica al derecho penal sustantivo que, a su vez, se subdivide en cinco títulos. El contenido de esta sección del Convenio permite apreciar la forma en que el legislador internacional decidió agrupar las conductas que deben ser sancionadas (Lezertua Rodríguez, 2001):

- Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos.
- Delitos informáticos.

- Delitos relacionados con el contenido.
- Delitos relacionados con infracciones de la propiedad intelectual y derechos afines.
- Otras formas de responsabilidad y sanción.

En concreto, en el título primero del Convenio sobre la Ciberdelincuencia se abordan los delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos. Es así que, el artículo segundo se centra en el acceso ilícito, que restringe las medidas de seguridad con el objetivo de obtener datos informáticos o cometer algún ilícito. El artículo tercero se refiere a la interceptación ilícita (deliberada e ilegítima) efectuada por medios técnicos. Es decir, el acceso no autorizado a sistemas de comunicación y transmisiones electrónicas (Morales García, 2002).

El artículo cuarto se enfoca en los ataques a la integridad de los datos. En su primer párrafo el legislador internacional configura un delito que exige la causación de un resultado concreto para poder apreciarse (dañar, borrar, deteriorar, alterar o suprimir). En las palabras exactas del Convenio sobre la Ciberdelincuencia (2001): “cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de actos que dañen, borren, deterioren, alteren o supriman datos informáticos” (artículo 4.1).

En el segundo párrafo del artículo cuarto se puede apreciar que el legislador internacional otorga a los Estados una reserva respecto a los ataques a la integridad de los datos. Así, se les reconoce la capacidad para que decidan si exigen, además de las conductas del primer párrafo, que el tipo penal sólo sea aplicable cuando con ellas se produzca un resultado grave. Sin embargo, no especifica los parámetros con los que interpretar dicha gravedad.

En el artículo quinto el Convenio sobre la Ciberdelincuencia (2001) refiere a los ataques a la integridad del sistema. Por lo cual, los artículos cuarto y quinto dan cuenta de la intención de armonizar las cuestiones relacionadas con los daños informáticos. De este modo, el artículo

cuarto se concentra en la intercepción de datos y el artículo quinto en la interferencia en sistemas informáticos. En el mismo sentido, el mandato del legislador nacional interpela a regular aquellas situaciones en las que se produzca un resultado concreto: la obstaculización. Igualmente, la intercepción tiene un carácter grave, deliberado e ilegítimo en el funcionamiento de un sistema informático (González Hurtado, 2013).

En realidad, el Convenio tiene como objetivo penalizar las conductas graves que afecten a los datos informáticos o a los sistemas. Pero, la técnica legislativa que se utiliza difiere entre ambos artículos. En el caso del artículo cuarto se establece el delito sin mencionar inicialmente la gravedad del resultado. Posteriormente, se permite a los legisladores de los Estados decidir sobre cuando dicho resultado es de gravedad. Por su parte, el artículo quinto requiere, específicamente, que la obstrucción sea grave. Así, reconoce, igualmente, a los Estados la regulación de la conducta en todos los casos, no solo en los más graves.

Además de lo mencionado anteriormente, es adecuado el análisis de algunos puntos adicionales. En primer lugar, en términos de la tipificación de las acciones relevantes desde una perspectiva penal, se observa la inclusión simultánea de dos conductas con elementos similares. Esto sugiere que, aunque son acciones distintas, ambas tienen como objetivo proteger, primordialmente, los mismos elementos: la defensa de la propiedad de bienes intangibles. En efecto, se regulan los daños de manera amplia a la vez que se dividen en dos categorías distintas. En el artículo cuarto se sanciona el daño directo a bienes específicos del sujeto pasivo. Por su parte, en el artículo quinto se señala el perjuicio causado por la incapacidad para utilizar un objeto (el sistema informático en su totalidad) (De La Cuesta Arzamendi y De La Mata Barranco, 2010).

Además, el Convenio establece la necesidad de condenar penalmente el abuso de dispositivos. En este orden, se incluye la producción, venta, obtención, importación o difusión de dispositivos o programas informáticos diseñados para cometer los delitos descritos en los

artículos mencionados. Incluso, el caso de contraseñas o códigos de acceso a datos informáticos que faciliten el acceso ilegal a sistemas informáticos para perpetrar cualquiera de las acciones delictivas descritas desde el artículo segundo al quinto.

El artículo sexto del Convenio sobre Ciberdelincuencia de Budapest (2001) trata sobre el abuso de dispositivos. El mismo se enfoca en la criminalización de la producción, venta, distribución, importación, difusión de dispositivos o programas informáticos. Es decir, se refiere a la tipificación del abuso de los dispositivos diseñados para cometer los delitos descritos en los artículos anteriores. Además, abarca la penalización de la obtención, posesión o uso de contraseñas o códigos de acceso a sistemas informáticos con la intención de cometer delitos.

La sección dedicada al Derecho sustantivo continúa con el título segundo denominado delitos informáticos. De este modo, se refiere a las acciones de falsificación informática (artículo séptimo) y fraude informático (artículo octavo). Sobre la falsificación informática sostiene que es el delito relacionado con la introducción, alteración, borrado o supresión en forma deliberada e ilegítima de datos informáticos. Y, precisamente, que a través de esta acción se tenga la intención de que sean tomados o utilizados como auténticos en términos legales.

Por lo que se refiere al fraude informático, el Convenio establece la tipificación de los actos deliberados e ilegítimos que causen daño patrimonial a una persona. Y, que mediante esta acción se tenga la intención delictiva de obtener información no autorizada para conseguir un beneficio económico. En la comisión del fraude informático se consideran dos vertientes, por un lado, la introducción, alteración, borrado o supresión de datos informáticos. Por otra parte, la realización de cualquier interferencia en el funcionamiento de un sistema informático.

En el título tercero de la sección primera el Convenio aborda aquellos delitos relacionados con el contenido informático. En esta línea, exclusivamente señala los delitos relacionados con la pornografía infantil. En el párrafo segundo define que se comprende a todo

material pornográfico que contenga la representación visual de un menor o una persona que parezca un menor adoptando un comportamiento sexual explícito. Incluso, se caratula como pornografía infantil a las imágenes realistas que representen a un menor adoptando un comportamiento sexual explícito. A continuación, en el párrafo tercero se expresa que el menor es toda persona con menos de 18 años o, según la decisión de cada país, el límite de edad puede ser hasta los 16 años. Todavía cabe señalar que en el párrafo primero se insta a los Estados que tipifiquen como delito la comisión de los siguientes actos:

- La producción, la oferta o la puesta a disposición de pornografía infantil con la intención de difundirla a través de un sistema informático.
- La difusión o la transmisión de pornografía infantil a través de un sistema informático.
- La adquisición, para uno mismo o para otros, de pornografía infantil a través de un sistema informático.
- La posesión de pornografía infantil en un sistema informático o en un dispositivo de almacenamiento de datos informáticos.

En el título cuarto de la sección dedicada al Derecho sustantivo recoge los delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines. Por su parte, el título quinto aborda las formas de comisión y la responsabilidad de las personas jurídicas, que no siempre debe ser de naturaleza penal. Se salva así el inconveniente que supone, en algunas regulaciones de los Estados Parte, la falta de responsabilidad penal de las personas jurídicas en sus sistemas legales. Además, en este último título de la sección primera se estipulan los requisitos que deben cumplir las sanciones establecidas en las regulaciones internas para cumplir con las disposiciones del Convenio (Silva Sánchez, 2002).

> Cada parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para que pueda exigirse responsabilidad a las personas jurídicas por los delitos previsto en una aplicación del presente Convenio, cuando éstos sean cometidos por cuenta de las

> mismas por una persona jurídica, ya sea a título individual o como miembro de un órgano de dicha persona jurídica, que ejerza funciones directivas en su seno, en virtud de: a) un poder de representación de la persona jurídica; b) una autorización para tomar decisiones en nombre de la persona jurídica; c) no autorización para ejercer funciones de control en el seno de la persona jurídica (Convenio sobre Ciberdelincuencia, 2001, artículo 12.1).

Así, en el artículo décimo primero se solicita a los Estados que tipifiquen en sus legislaciones internas la complicidad deliberada en relación con los delitos descritos en los artículos anteriores del Convenio. Sin embargo, se debe mencionar que el Convenio adopta una postura más flexible respecto a la tipificación de la tentativa. Por consiguiente, recomienda su adopción en los delitos comprendidos en los artículos 3, 4, 5, 7, 8, 9.1.a, 9.1.c. Aunque, no se exige de manera categórica, como se desprende de la cláusula del artículo 11.3 que otorga libertad a los Estados para aplicar este extremo (González Hurtado, 2013).

El artículo decimotercero refiere a las sanciones y medidas legislativas que los Estados parte deben adoptar para los delitos previstos en los artículos anteriores. Para que, de esta forma, frente a las acciones ilícitas se impongan sanciones efectivas, proporcionadas y disuasorias. Así, se insta a la aplicación de sanciones o medidas penales o no penales. Inclusive, las penas privativas de la libertad y las sanciones pecuniarias.

A continuación, inicia la sección segunda del capítulo segundo que se extiende desde el artículo décimo cuarto hasta el vigésimo primero. Más precisamente, el Convenio sobre Ciberdelincuencia (2001) detalla el derecho procesal. De manera similar a la sección de los delitos tipificados en la sección primera, los Estados se encuentran obligados a incorporar en sus sistemas internos los procedimientos y especificaciones del Convenio.

Además, se demanda a los Estados parte la protección adecuada de los derechos humanos y las libertades individuales en consonancia con otros instrumentos internacionales

existentes. Específicamente, menciona el Convenio del Consejo de Europa para la protección de los derechos humanos y las libertades fundamentales (1950) y el Pacto Internacional de derechos civiles y políticos de las Naciones Unidas (1966) (Pérez Gil, 2004; Velasco Núñez, 2006).

Los procedimientos establecidos en las legislaciones procesales de los Estados Parte tienen como objetivo principal estandarizar la conservación de los datos informáticos (artículo décimo sexto) y también la conservación y revelación parcial rápida de datos de tráfico (artículo décimo séptimo). Asimismo, se estipula la emisión de órdenes de comunicación e información por parte de las autoridades (artículo décimo octavo).

Además, se manda el establecimiento de procedimientos de registro y confiscación de datos informáticos almacenados. Para que, de esta forma, se faculte a las autoridades competentes a registrar o tener acceso de modo similar a todo sistema informático o dispositivo de almacenamiento informático (artículo décimo noveno). Igualmente, se insta a adoptar las medidas necesarias para la obtención en tiempo real de datos de tráfico (artículo vigésimo) y la interceptación de datos relativos al contenido (artículo vigésimo primero).

En la sección tercera, y última del capítulo tercero, se manda que cada Estado parte debe adoptar las medidas necesarias para afirmar su jurisdicción respecto de cualquier delito previsto entre los artículos segundo al décimo primero. Más precisamente, se refiere al delito que se haya cometido: en su territorio, a bordo de un buque que enarbole su pabellón, a bordo de una aeronave matriculada según sus leyes o por uno de sus nacionales (en caso de que el delito sea susceptible de sanción penal en el lugar que se cometió o si ningún Estado tiene competencia territorial respecto del mismo) (Convenio sobre Ciberdelincuencia, 2001).

Luego, se erige el capítulo tercero dedicado al aspecto de la cooperación internacional y se subdivide en dos secciones: principios generales y disposiciones específicas. En este sentido, observa las recomendaciones de los instrumentos internacionales sobre delincuencia

informática existentes y actúan en continuidad. Para, de este modo, sentar las bases de regulación de los métodos de cooperación internacional en el tratamiento de la ciberdelincuencia. Es por ello, que el capítulo tercero se relaciona estrechamente con las secciones segunda y tercera del capítulo anterior.

Así, el capítulo tercero se centra en la cooperación internacional para la persecución de delitos informáticos y la situación de adhesión de los Estados al mismo (Foggetti, 2003; Rodríguez Bernal, 2007). En definitiva, el objetivo es mejorar las posibilidades de persecución y enjuiciamiento de los autores de los delitos descritos en la sección primera del capítulo segundo. Al respecto, Pérez Gil (2004) analiza las normas procesales del Convenio sobre Ciberdelincuencia (2001) a la luz de la jurisprudencia del Tribunal Europeo de Derechos Humanos (TEDH) en los siguientes ámbitos:

- El requerimiento de aportación o exhibición de datos informáticos donde la doctrina del TEDH protege al acusado y su derecho a no autoincriminarse. Así, permite rechazar dicho requerimiento, excepto cuando se dirige a un tercero en el proceso.
- El registro e incautación de sistemas y datos informáticos, considerados medios de aseguramiento de la prueba, que seguirán las reglas comunes de registro e incautación de elementos del delito.
- La intervención de comunicaciones electrónicas, sobre las que el TEDH insiste en la necesidad de establecer reglas claras y detalladas, en línea con la doctrina establecida para las intervenciones telefónicas.

Particularmente, la sección primera del capítulo tercero se refiere a los principios generales y relativos a la cooperación internacional, a la extradición, a la asistencia mutua, a la información espontánea, a las reglas aplicables cuando no existan acuerdos internacionales, y también a la confidencialidad y restricciones de uso. En cuanto al artículo vigésimo tercero y

cuarto González Hurtado (2013) es crítico: “El capítulo introduce pocas novedades destacables respecto a los principios generales de cooperación (artículo 23) y de extradición (artículo 24)”.

Se compele a los Estados Partes a que dediquen esfuerzos a la cooperación mediante la aplicación de los instrumentos internacionales en materia penal. Así como también de los acuerdos basados en legislación uniforme o recíproca y de su derecho interno. En relación con la extradición, se delinean directrices generales para los delitos cuya pena sea privativa de libertad por más de un año. Esto es, siempre de manera supletoria a los tratados de extradición firmados al margen del Convenio sobre Ciberdelincuencia (2001) y al derecho interno de cada Estado. Al mismo tiempo, se regula la solución de controversias en materia de extradición.

En cambio, desde los artículos vigésimo quinto al trigésimo cuarto el Convenio enumera en detalle los procedimientos y límites de la asistencia mutua en las labores de investigación y prevención. A su vez, insta a los Estados parte a efectuar las reformas legislativas necesarias para cumplir con las medidas que se extienden en la sección primera y segunda del capítulo tercero. De acuerdo a Sánchez Siscart (2011) se puede clasificar las medidas que los Estados deben regular en sus ordenamientos internos de la siguiente manera:

- Preservación urgente de datos informáticos almacenados (artículo 29).
- Revelación urgente de datos de tráfico almacenados (artículo 30).
- Acceso a datos informáticos almacenados (artículo 31).
- Acceso transfronterizo a datos almacenados, con consentimiento o cuando estén a disposición del público (artículo 32).
- Asistencia mutua para la obtención en tiempo real de datos sobre el tráfico (artículo 33).
- Asistencia mutua relativa a la interceptación en tiempo real de datos sobre el contenido (artículo 34).
- Transmisión espontánea de información (artículo 26).

- Creación de red de puntos de contactos permanente denominados ‘Red 24/7’ (artículo 35).

En lo referido a la asistencia mutua, el artículo vigésimo quinto refiere a que los Estados deben prestar toda ayuda mutua en las investigaciones o en los procedimientos relativos a delitos informáticos. En este marco, González Hurtado (2013) destaca que el Convenio propicia la eliminación de trámites burocráticos excesivos para la solicitud de aquella. Para ilustrar mejor, se puede mencionar que se permite en los casos de urgencia el envío de un correo electrónico entre las Partes. Es decir, se trata de la utilización de medios de comunicación que sean rápidos y que, al mismo tiempo, ofrezcan niveles suficientes de seguridad y de autenticación.

Por lo que se refiere a la ausencia de acuerdos internacionales sobre asistencia mutua, las disposiciones del Convenio establecen procedimientos que se ocupen de estos casos. De este modo, se estipula que los Estados Parte deben designar una autoridad central responsable de la asistencia mutua con la función de velar por el cumplimiento del Convenio y de su derecho aplicable. Además, en los casos urgentes se prevé que la autoridad judicial tiene la capacidad de solicitar directamente la asistencia. En este artículo, vigésimo séptimo, también se considera:

- La denegación de asistencia: en casos que se trate de delitos políticos o cuando la asistencia pueda atentar contra la soberanía, la seguridad, orden público u otros intereses esenciales de los Estados (artículo 27.4).

- La suspensión de asistencia en casos que pueda causar perjuicios a otras investigaciones en marcha (artículo 27.5)

- La solicitud de utilizar los datos facilitados en virtud de la asistencia de forma confidencial (artículo 27.8 y se profundiza en el subsiguiente artículo 28).

En la sección segunda del capítulo tercero se establecen pautas comunes sobre la conservación rápida de datos almacenados en sistemas informáticos. Así, en el artículo vigésimo noveno se establecen las pautas que un Estado Parte debe seguir cuando solicita a otro la conservación rápida de datos que se encuentren en su territorio. Y, a continuación, se regula la revelación rápida de datos conservados en relación con la conservación:

> Si, al ejecutar una solicitud formulada de conformidad con el artículo 29 para la conservación de datos relativos al tráfico de una determinada comunicación la Parte requerida descubriera que un proveedor de servicios de otro Estado ha participado en la transmisión de dicha comunicación, dicha Parte revelará rápidamente a la Parte requirente un volumen suficiente de datos relativos al tráfico para que pueda identificarse al proveedor de servicios, así como la vía por la que la comunicación ha sido transmitida (Convenio sobre Ciberdelincuencia, 2001, artículo 30.1).

En cuanto a la asistencia mutua en relación con el acceso a datos almacenados, el Convenio permite que entre Estados Parte se puedan solicitar el registro, obtención o la revelación de datos almacenados por medio de un sistema informático. Asimismo, se regula el acceso transfronterizo a datos almacenados, con consentimiento o cuando sean accesibles al público. En esta línea, según el artículo trigésimo segundo un Estado parte puede sin necesidad de autorización:

- Tener acceso a datos informáticos almacenados accesibles al público (fuente abierta) independientemente de la ubicación geográfica de los mismos.
- Tener acceso a datos informáticos almacenados en otro Estado, o recibirlos, a través de un sistema informático situado en su territorio, si dicha Parte obtiene el consentimiento lícito y voluntario de la persona legalmente autorizada a revelarlos por medio de ese sistema informático.

En relación con la asistencia mutua para la obtención en tiempo real de datos relativos al tráfico y al contenido el Convenio estipula la asistencia mutua para su consecución. Es decir, aquellos datos relativos al tráfico y al contenido asociados a comunicaciones específicas transmitidas por medio de un sistema informático. De acuerdo con lo analizado en estos últimos artículos, y sobre el capítulo tercero, cabe advertir el nivel de detalle con que el Convenio regula la asistencia mutua.

Todavía cabe profundizar en que el Convenio constituye la Red 24/7 que, tal como manifiesta su denominación, "supone un punto de contacto para la prestación de ayuda inmediata en orden a la realización de investigaciones relacionadas con los delitos informáticos que deberá encontrarse operativa en todo momento" (González Hurtado, 2013, p. 94). A estos efectos, la Red 24/7 tiene como objetivo: "garantizar una asistencia inmediata para investigaciones relativas a delitos vinculados a sistemas y datos informáticos, o para obtener las pruebas en formato electrónico de un delito" (Convenio sobre Ciberdelincuencia, 2001, artículo 35). Más precisamente, la Red 24/7 tiene como funciones principales (Sánchez Siscart, 2011):

- El asesoramiento técnico
- La conservación de datos en aplicación de los artículos 29 y 30
- La obtención de pruebas, el suministro de información jurídica y la localización de sospechosos.

La existencia de este capítulo sobre la cooperación internacional es crucial para el abordaje de la delincuencia informática, más allá de que su aplicación efectiva puede ser complicada. Uno de los mayores desafíos en la persecución de la delincuencia informática es la dificultad de prevenir el delito, ya que la intervención de las autoridades judiciales y policiales suele ocurrir después de que se efectuaron los daños. Así, la problemática acentúa la necesidad de articular un método eficaz de investigación. Así como también la puesta a

disposición de los autores de delitos informáticos entre los Estados para evitar que estos ataques se repitan.

Otras cuestiones paralelas a la dificultad de aplicación de este Convenio son advertidas por autores como Pérez Gil (2004) y Sánchez Bravo (2002). Ambos autores estiman que la aprobación de este Convenio representa un hito en los ámbitos penal y procesal. Y, al mismo tiempo, concuerdan en la preocupación de que, excesivamente, tenga lugar la priorización de la seguridad nacional sobre la privacidad personal. En otras palabras, de que el Convenido no debe servir como excusa para una desde la esfera gubernamental se invada la esfera privada de los ciudadanos sin el adecuado control jurisdiccional.

Finalmente, el capítulo cuarto trata sobre las Disposiciones Finales similares a las de otros Convenios del Consejo de Europa. En estas cláusulas generales se abordan aspectos como la entrada en vigor, la adhesión de otros países, la aplicación territorial, los efectos del Convenio y otras cláusulas relacionadas con reservas, declaraciones y enmiendas (Acurio Del Pino, 2015). Así, en el artículo trigésimo sexto se establece la apertura del Convenio para la firma de los Estados miembros del Consejo de Europa y de los Estados no miembros que participaron en su elaboración.

También se especifica que dado el caso de que dos o más Estados partes del Convenio firmen otro relativo a la ciberdelincuencia, el contraído en Budapest solamente regirá subsidiariamente. Aunque, siempre y cuando las normas no resulten incompatibles con las disposiciones de éste. El Convenio establece el procedimiento para ser enmendado. En lo que se refiere a la cláusula federal permite el derecho de reservarse de cumplir las obligaciones del capítulo segundo del Convenio a condición de que puedan garantizar la cooperación internacional. Por otro lado, cuando los Estados Parte en controversia no puedan llegar a un acuerdo se insta a la solución mediante un tribunal de arbitraje.

2.4.1. Primer Protocolo adicional al Convenio sobre la ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos

El Convenio sobre la Ciberdelincuencia (2001) se complementa con un Primer Protocolo Adicional (2003). En concreto, se trata de un documento que profundiza en la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos. De este modo, el Protocolo Adicional aborda temas que no se enfatizaron en el año 2000 y que están estrechamente relacionados con la ciberdelincuencia. Así, se pretende armonizar la lucha contra el racismo y la xenofobia en los sistemas de información y las redes de comunicaciones (Pavón Pérez, 2003).

De acuerdo al Consejo de Europa (2024), el Primer Protocolo Adicional cumple el cometido de ampliar el ámbito de aplicación del Convenio sobre la Ciberdelincuencia. En particular, porque incluye disposiciones sustantivas, procesales y de cooperación internacional sobre los delitos de propaganda racista o xenófoba cometidos en medios informáticos. De esta manera, el Primer Protocolo Adicional armoniza los elementos de derecho sustantivo de estas conductas y mejora la capacidad de los Estados Partes para la cooperación internacional. Especialmente, señala que las ventajas son:

- Un marco jurídico más sólido: refuerza el marco legal que combate la xenofobia y el racismo en el ciberespacio. Así también, proporciona pautas claras para la tipificación de estos delitos cometidos por medios informáticos.
- Mayor cooperación internacional: propicia la cooperación internacional en la investigación y persecución de delitos vinculados con la xenofobia y el racismo en línea. Así, su relevancia tiene que ver con el carácter transfronterizo de muchos de estos ilícitos.
- Mayor protección para las víctimas: la penalización de la xenofobia y el racismo en línea permite a las víctimas buscar justicia y recibir apoyo.

El Primer Protocolo Adicional se destaca como un avance en la materia que complementa al Convenio sobre la Ciberdelincuencia (2001). Al mismo tiempo, algunos autores sostienen que su adopción no completa la totalidad de conductas que debieran ser objeto de atención. Es decir, en perspectiva de una completa lucha contra lo que forma parte del concepto cibercrimen. Explícitamente, "quedan extramuros del mismo aquellas otras [conductas], igualmente discriminatorias, de otra naturaleza (así, por ejemplo, en relación a supuestos de discriminación sexual o de discriminación motivada por deficiencias físicas o psíquicas)" (De La Cuesta Arzamendi y De La Mata Barranco, 2010, p. 134).

2.4.2. Segundo Protocolo Adicional al Convenio sobre la Ciberdelincuencia, relativo a la cooperación reforzada y la divulgación de pruebas electrónicas

En complemento al Convenio sobre la Ciberdelincuencia (2001) tiene lugar el Segundo Protocolo Adicional sobre la Ciberdelincuencia, relativo a la cooperación reforzada y la divulgación de pruebas electrónicas (2022). En esta ocasión se consideró la problemática de la proliferación de la ciberdelincuencia y la creciente complejidad en la obtención de pruebas electrónicas. Particularmente, porque las pruebas electrónicas se pueden almacenar en jurisdicciones extranjeras, múltiples, cambiantes o desconocidas.

Asimismo, las competencias de las autoridades de justicia penal se ven limitadas por las fronteras territoriales frente a la naturaleza transnacional de los delitos informáticos. De esta forma se ve comprometido su abordaje dado que solo una pequeña fracción de la ciberdelincuencia denunciada a las autoridades policiales suele culminar en decisiones judiciales. En respuesta a este desafío, el Segundo Protocolo Adicional instituye una base jurídica para la divulgación de información sobre el registro de nombres de dominio.

También, el Segundo Protocolo Adicional estipula una base jurídica para la cooperación directa con los proveedores de servicios respecto a la información de sus abonados. Además,

introduce medios eficaces para la obtención de información sobre abonados y datos de tráfico, cooperación inmediata en casos de emergencia, herramientas de asistencia mutua y salvaguardias para la protección de datos personales (Consejo de Europa, 2024).

Entre las principales características del Protocolo se encuentran:

- Solicitudes directas a registradores de otras jurisdicciones para obtener información sobre el registro de nombres de dominio.
- Órdenes directas a proveedores de servicios de otras jurisdicciones para obtener información sobre los abonados.
- Medios más eficaces para obtener información sobre abonados y datos de tráfico mediante la cooperación entre gobiernos.
- Cooperación expedita en situaciones de emergencia.
- Equipos conjuntos de investigación e investigaciones conjuntas.
- Uso de videoconferencias.

2.5. Regulación en el ámbito europeo

2.5. 1. La recomendación R(89)9 del Consejo de Europa

La recomendación R(89)9 del Consejo de Europa (1989) se conformó como una herramienta de gran influencia a nivel internacional en la regulación de los delitos informáticos. Cabe considerar que para ese entonces la ONU no abordaría este tema hasta su Octavo Congreso en 1990. Por tanto, la recomendación R(89)9 solamente tiene como punto de partida los trabajos previos realizados en el marco de la OCDE (Lezertua Rodríguez, 2001).

En pleno impacto revolucionario de las tecnologías de la información la recomendación R(89)9 da cuenta de sus aspectos positivos y negativos. Es decir, tanto de los beneficios y ventajas como de los abusos y el crimen que derivan de las tecnologías de la información. Así,

tras una introducción que repasa los antecedentes de la OCDE, desarrolla un documento exhaustivo desde diversas perspectivas sobre el delito informático.

El contenido de la recomendación R(89)9 se divide en cinco puntos principales. El primero contextualiza el fenómeno de la delincuencia informática en el contexto histórico propio de su surgimiento. El segundo punto se centra en la estipulación de un listado de conductas que estima deben ser consideradas como delictivas en la legislación interna de los Estados. Al respecto, González Hurtado (2013) destaca que la innovación significativa en comparación con la lista que elaboró la OCDE fue que la recomendación R(89)9 presentó dos listas de conductas delictivas:

- Una lista que enumera conductas que deberían ser consideradas delictivas sin excepción. En este orden, se reconocen dentro de la lista mínima: el fraude informático, la falsificación informática, daños a datos o programas informáticos, el sabotaje informático, el acceso ilícito, la interceptación ilícita y delitos contra la propiedad intelectual e industrial.
- Una lista que describe supuestos de regulación recomendada. Se trata de una lista opcional de conductas a regular que incluye: la alteración de datos o programas informáticos, el espionaje informático, la utilización de un ordenador sin consentimiento de su titular y la utilización de un programa informático sin el consentimiento de su titular.

En este segundo punto es importante tener en cuenta que la recomendación R(89)9 no tiene carácter vinculante. En consecuencia, la clasificación de las conductas merecedoras de reproche penal en una lista u otra no afecta directamente a las políticas de los Estados que buscan regular los delitos informáticos. Sin embargo, se puede reconocer la virtud de que a través de este sistema de doble lista se otorgó mayor preocupación por ciertos tipos de conductas sobre otras. Así, la relevancia es la orientación de los esfuerzos legislativos hacia las materias incluidas en la lista mínima.

Por lo que se refiere al tercer punto, la recomendación R(89)9 hace énfasis en los desafíos que implica la persecución de los delitos informáticos. En el cuarto punto se abordan las problemáticas de jurisdicción y de aplicación del derecho penal ante el carácter transnacional de estos ilícitos.[6] Por último, el quinto punto se refiere a los aspectos vinculados con la protección de las víctimas de delitos informáticos y las medidas para prevenirlos (Lezertua Rodríguez, 2001).

2.5. 2. Las Conferencias Internacionales de la Universidad de Wurzburgo

En 1992 se celebraron tres conferencias internacionales en Wurzburgo (Alemania) organizadas por la Universidad local. En estos encuentros el foco estuvo en la recopilación y análisis de datos sobre la delincuencia informática a nivel internacional. Y, más precisamente, en estas reuniones se exploró el modo en que estos ilícitos se estaban incorporando en los sistemas legales internos. Por lo que, se analizó el abordaje alcanzado en gran cantidad de países y la dirección futura en esta área (Sieber, 1994). Las conferencias fueron organizadas por:

- La Asociación Internacional de Derecho Penal (AIDP) sobre "delitos informáticos y otros delitos relacionados con las tecnologías de la información."
- Las Comunidades Europeas sobre "fraude informático y legislación sobre delincuencia informática en las Comunidades Europeas."
- La ONU respecto de "la contribución de las Naciones Unidas a la persecución y prevención de los delitos informáticos."

El resultado final de las tres conferencias internacionales fue un estudio exhaustivo y completo hasta esa fecha. Así como otros esfuerzos en la materia, se subrayó la creciente

[6] Sobre este aspecto, en 1995 se elaboró otra recomendación específica acerca del modo en que los Estados deberían actuar para perseguir los delitos informáticos.

importancia y naturaleza transnacional de los delitos informáticos. Se relevaron las medidas adoptadas por el Consejo de Europa, la ONU y, en menor medida, las Comunidades Europeas. Además, la AIDP analizó detalladamente las legislaciones penales implementadas en más de veinticinco naciones (Gutiérrez Francés, 2005).

En suma, se puede advertir que las conferencias de 1992 devinieron en una especie de enciclopedia que recapitula la situación de la delincuencia informática en ese contexto histórico. Sobre todo, su utilidad fue conformarse como un recurso fundamental para la investigación y las propuestas que serían la base del trabajo de la década siguiente. En especial, para uno de los organismos que participó de las conferencias internacionales: la ONU: "Especialmente relevante para los trabajos de la ONU tanto en su Manual publicado en 1994, como para los posteriores Congresos sobre prevención del delito y tratamiento del delincuente" (González Hurtado, 2013, p. 70).

De manera análoga, los efectos se pueden encontrar en un nuevo impulso legislativo de los Estados europeos. Aunque este crédito no se cita explícitamente en los trabajos legislativos de aquellos, se puede encontrar una cierta relación con la publicación de los trabajos de las conferencias. En concreto, en los esfuerzos por armonizar las regulaciones penales de los ordenamientos internos. Justamente, en los coloquios las recomendaciones contemplaron que el derecho penal tradicional empezaba a ser insuficiente para el abordaje de los nuevos desafíos informáticos. Por consiguiente, las recomendaciones que surgieron de las conferencias internacionales promocionaron la reforma de los delitos existentes y la creación de otros nuevos. Las recomendaciones enfatizaban la importancia de que las nuevas disposiciones fueran precisas y claras. Así como también la limitación de la responsabilidad penal a actos deliberados considerando la rápida evolución tecnológica y conceptual en el ámbito informático.

Con especial atención al valor de los bienes intangibles de la informática y las potenciales implicaciones delictivas del avance tecnológico, se sugirió a los Estados la tipificación de delitos punibles en la materia. Tales recomendaciones se efectuaron contemplando que cada país tiene sus tradiciones jurídicas y culturales y distintas posibilidades de aplicabilidad de acuerdo a su legislación vigente. Entre las conductas punibles se destacan las relativas a la alteración de datos informáticos, el espionaje informático y el delito de acceso no autorizado. Igualmente, se subrayó la necesidad de considerar punibles el tráfico de contraseñas informáticas obtenidas de manera inapropiada y la distribución de virus u otros programas similares (Acurio Del Pino, 2016).

2.5.3. Decisión 92/242/CEE del consejo, de 31 de marzo, en materia de seguridad de los sistemas de información

La Decisión 91/242/CEE del 31 de marzo de 1992 constituyó uno de los primeros instrumentos sobre la seguridad informática en el ámbito europeo. Más precisamente, en el organismo supranacional que en ese momento era la Comunidad Económica Europea. Por consiguiente, forma parte de los esfuerzos precursores en la materia en línea con los trabajos de otros organismos internacionales en los albores de la década de 1990. Cabe destacar que se adoptó una medida en el campo de la seguridad de los sistemas de información que incluía dos elementos principales:

- Plan de acción para la seguridad de los sistemas de información durante un periodo de 24 meses. En concreto, el objetivo era el desarrollo de estrategias globales destinadas a la protección adecuada contra amenazas accidentales o deliberadas. Para ello, se delineaban pautas o estrategias dirigidas a los usuarios y productores de información almacenada, procesada o transmitida electrónicamente. El plan de acción se debía realizar en estrecha

colaboración con los actores del sector informático. Para su ejecución, se debían considerar las actividades en curso a nivel internacional para la armonización en este ámbito.

- La creación de un Comité de altos funcionarios con el objetivo a largo plazo de asesoramiento a la Comisión sobre acciones en materia de seguridad de los sistemas de información. En este orden, se estableció que el Comité sería consultado sistemáticamente por la Comisión acerca de las distintas actividades que ésta última realizaba. En particular, sobre lo relativo a la definición de las estrategias y los programas de trabajo.

Además de lo mencionado, en la elaboración del plan de acción o desarrollo de estrategias globales debía incluirse:

- El desarrollo de un marco estratégico para la seguridad de los sistemas de información.
- La definición de las necesidades de los usuarios y de los prestadores de servicios en materia de seguridad de los sistemas de información.
- La elaboración de soluciones para determinadas necesidades a corto y medio plazo de los usuarios, proveedores y prestadores de servicios.
- La elaboración de especificaciones, normas y pruebas de certificación respecto a la seguridad de los sistemas de información.
- Las innovaciones técnicas y de funcionamiento en materia de seguridad de los sistemas de información en un marco estratégico general y, finalmente.
- La puesta en práctica de la seguridad de los sistemas de información.

De acuerdo a González Hurtado (2013) la Decisión 91/242/CEE (1992) demostró por primera vez el interés genuino de la Comunidad Económica Europea por la seguridad informática. En especial, la voluntad de armonizar y asegurar que a la par de la evolución vertiginosa de las tecnologías de la información se garantizara su uso seguro por parte de todos los Estados miembros. Aunque, en términos de su materialización, el texto de la Decisión evidencia la ausencia de referencias al ordenamiento penal que debían seguir las partes.

Justamente, porque se encuadrada en las competencias que la Comunidad Económica Europea tenía en ese momento. En efecto, ni el Tratado Constitutivo de la Comunidad Económica Europea (1957) ni sus revisiones posteriores revistieron de poderes en materia penal al organismo supranacional. Recién con el Tratado de la Unión Europea (1992) se amplió relativamente la competencia para poder regular en este ámbito con los principios de cooperación en lo relativo a la justicia y asuntos de interior. Y, sustancialmente, el Tratado de Ámsterdam (1997) consagra el denominado espacio de libertad, seguridad y justicia (Calonge Velázquez, 2006; Rodríguez Bernal, 2007). En este proceso, Bacigalupo Saggese (2005) señala que con la Constitución Europea se ampliaron las competencias penales respecto a delitos como el terrorismo, la trata de seres humanos o la delincuencia informática, entre otros.

Visto en perspectiva, no resulta sorprendente la ausencia de disposiciones directas concernientes a la legislación penal de los Estados miembros en la Decisión 91/242/CEE (1992). Más allá de esta cuestión, los primeros pasos cumplieron la finalidad de dar curso a la observación activa de la delincuencia informática en el ámbito europeo y establecer órganos consultivos de expertos en la materia. Por lo que, en términos generales, este documento fue importante desde el punto de vista de la política común y la acción de la Comunidad Económica Europea en materia de seguridad de los sistemas de información. A partir de entonces se despertó una preocupación constante de las instituciones europeas por abordar la seguridad informática.

2.5. 4. II Jornadas Internacionales sobre el Delito Cibernético

Las II Jornadas Internacionales sobre el Delito Cibernético (1998) fueron organizadas por la Universidad Nacional de Educación a Distancia de España. En estas Jornadas se reunieron numerosos especialistas del ámbito jurídico, policial y político tanto de España como de otros países. De este modo, se constituyeron como una importante contribución a la

concientización en la materia desde la óptica de distintos ámbitos y quedaron publicados en una diversidad de temáticas.

Algunos especialistas trataron temas de carácter global relativos a la sociedad digital o de la información (Ribas Alejandro, 1998; Benedito Agramunt, 1998). Otros, especialistas hicieron énfasis en la delincuencia informática, bajo distintas denominaciones como ser delitos informáticos o delitos cibernéticos (Estrada Posada, R. y Somellera, 1998; Téllez Valdés, 1998). O, en términos más puntuales, en aspectos regulatorios de esta problemática, tanto en el derecho interno como en perspectiva supranacional (Ovilla Bueno, 1998; Jan Drijber, 1998; Carrascosa López, 1998).

Y, desde una perspectiva más concreta, se abordaron algunas conductas delictivas en el ámbito de la información y la necesidad de regulación para la protección de los usuarios (López Alonso, 1998). Se pueden mencionar ejemplificativamente temáticas como la protección de la intimidad, los contenidos ilícitos y nocivos de internet (Castillo Jiménez, 1998; Sánchez Bravo, 1998) Así como también, la economía digital y el lavado de dinero o la criptología, entre otros (Devoto, 1998; Molinea et al., 1998).

Del mismo modo, se profundizaron aspectos sobre el papel que las Fuerzas y Cuerpos de Seguridad del Estado debían ocupar en esa nueva estructura de persecución del delito informático transfronterizo (Atkins, 1998; Moral Torres, 1998). Así, se destacó la creciente necesidad de la cooperación policial internacional para la investigación de estos ilícitos (Swinburne, 1998; Vriesde 1998; Di Leone, 1998). Igualmente, acerca de los desafíos que el mundo digital representaba para la administración pública (Izquierdo Loyola, 1998).

En suma, las II Jornadas Internacionales sobre el Delito Cibernético (1998) reflejaron la creciente preocupación por la concientización o interés internacional sobre las tecnologías. Sobre todo, con su utilización para cometer ilícitos y la necesidad de regularlos adecuadamente. Fundamentalmente, se destacan las distintas vertientes que encauzaron la materia, desde el

ámbito administrativo o mercantil hasta el penal, jurisdiccional y policial. En este escenario, González Hurtado (2013) afirma que:

> El tiempo entre la implantación de Internet y los sistemas informáticos personales, y la concienciación de la necesidad de un adecuado marco regulatorio fue muy breve; otra cosa es el tiempo en que esa conciencia global se ha traducido en una regulación penal adecuada e igualmente global (p. 71).

2.5. 5. Comunicación sobre la necesidad de mejora de la seguridad de las infraestructuras de información de 2001

La COM(2000)890 final de 26 de enero de 2001 es la Comunicación de la Comisión de las Comunidades Europeas dirigida al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones. En concreto, se refiere a la necesidad de mejora de la seguridad de las infraestructuras de información en el contexto de la sociedad de la información y el abordaje de la problemática de los delitos informáticos.

En principio, la comunicación señala que el desarrollo de las tecnologías de la información y la comunicación provocaron cambios significativos y multidimensionales. Es decir, que impactaron directamente en el marco general del modelo de funcionamiento de la sociedad. De esta forma, ofrece oportunidades y amenazas, siendo crucial para el crecimiento, la competitividad y la creación de empleos en el continente europeo. Entre los puntos destacados, se subraya la relevancia de la seguridad de las redes de comunicaciones y la necesidad de afrontar los desafíos de la criminalidad informática.

La comunicación sostiene que la expansión de las infraestructuras de información y comunicación posibilitó nuevas conductas delictivas. En consecuencia, se requiere que la Unión Europea se plantee la adopción de una serie de medidas en el marco de su estrategia para combatir la delincuencia que utiliza la informática como medio. Justamente, define a la

delincuencia informática en un sentido amplio como “cualquier delito que de alguna manera implique el uso de tecnología de la información” (Comisión de las Comunidades Europeas, 2001, p. 12).

Además de conceptualizar la terminología, se refiere a otros conceptos análogos utilizados, como ser la delincuencia relacionada con la informática, la delincuencia de alta tecnología y la delincuencia cibernética. Al respecto, resuelve que todas las denominaciones tienen el mismo significado en la medida que todos comparten dos aspectos fundamentales. Por un lado, la explotación de las redes de información y comunicación sin ninguna dificultad geográfica. Y, por otro, dichos términos abordan a los delitos relativos a la circulación de datos intangibles y volátiles. Además, diferencia entre los delitos informáticos específicos y los delitos tradicionales perpetrados con ayuda de la informática:

> Un ejemplo típico se encuentra en el ámbito aduanero, donde Internet se utiliza como instrumento para cometer delitos típicos contra la normativa de aduanas, tales como el contrabando, la falsificación, etc. Mientras que los delitos informáticos específicos requieren una actualización de las definiciones de los delitos en los códigos penales nacionales, los delitos tradicionales perpetrados con ayuda de la informática requieren una mejora de la cooperación y de las medidas procesales (Comisión de las Comunidades Europeas, 2001, p. 12).

En la Comunicación se mencionan cuestiones relativas al derecho sustantivo para garantizar protección para las víctimas de la delincuencia informática. Así como también refiere a la asistencia jurídica mutua en una investigación penal y la necesidad de que la Unión Europea pueda tomar medidas efectivas en la materia. Asimismo, la Comunicación sostiene que la misma naturaleza de los delitos informáticos suponen un reto a las normas de derecho procesal penal. De este modo, enfatiza sobre el carácter transnacional, la velocidad, movilidad

y flexibilidad de los delitos informáticos y la intervención de distintas soberanías, jurisdicciones y normativas. En las cuestiones de derecho procesal se aborda:

- La interceptación de las comunicaciones.
- La retención de datos sobre tráfico.
- El acceso y uso son anónimos.
- La cooperación práctica a escala internacional.
- Las competencias de derecho procesal y jurisdicción.
- El valor probatorio de los datos informáticos.

En la Comunicación se establecieron una serie de medidas no legislativas que se centraron en la armonización de las disposiciones internas de los Estados en materia de delincuencia informática. Se sostiene la creación de unidades nacionales especializadas en la persecución y prevención del delito y la formación continua y especializada de policías y personal de la administración de justicia.

En otra de las medidas no legislativas se propone el desarrollo de instrumentos adecuados para el análisis estadístico de la delincuencia informática. Es decir, el mejoramiento de la información y de las normas comunes sobre mantenimiento de archivos. En un cuarto punto, se plantea la cooperación entre diversos actores mediante la creación de un Foro Europeo. Asimismo, se promueve la acción directa de las empresas para combatir la delincuencia informática. Por último, se delinea la realización de proyectos de investigación y desarrollo tecnológico financiados por el presupuesto de la Unión Europea (Comisión de las Comunidades Europeas, 2001).

Esta Comunicación encauza el proceso de evolución de la política común con un marcado aumento en el marco de la Unión Europea. Más concretamente, en áreas como la cooperación e investigación que se profundizaron en la posterioridad de la comunicación. Por tanto, si bien la COM(2000)890 es un instrumento menor dentro de la Unión Europea, es

importante en tanto se conformó como el punto de partida fundamental para la regulación penal y fiscal que se desarrolló a sus efectos (González Hurtado, 2013).

2.5. 6. Decisión Marco 2005/222/JAI del Consejo, de 24 de febrero de 2005

Tal como se mencionó en el apartado anterior, la Unión Europea persiste en la concertación de la política común de cooperación a nivel supranacional. Es claro, que un punto clave en este proceso lo constituye la Decisión Marco 2005/222/JAI relativa a los ataques contra los sistemas de información. Al igual que los instrumentos precursores, la Decisión Marco (2005) se propone mejorar la seguridad en la materia ante los desafíos de la delincuencia informática.

En particular consideración de su naturaleza transnacional, se plantea el fortalecimiento de la cooperación mediante la armonización de las normas penales. De este modo se pretende que los países de la Unión Europea puedan reprimir uniformemente los ataques contra los sistemas de información (Huete Nogueras, 2010; Rodriguez Bernal, 2007). Incluso, la Decisión Marco (2005) parte de la necesidad de homogeneizar el concepto de sistema de información para todos los Estados miembros:

> Todo aparato o grupo de aparatos interconectados o relacionados entre sí, uno o varios de los cuales realizan, mediante un programa, el tratamiento automático de datos informáticos, así como los datos informáticos almacenados, tratados, recuperados o transmitidos por estos últimos para su funcionamiento, utilización, protección y mantenimiento (Consejo de la Unión Europea, 2005, artículo 1).

A partir de la definición de sistema de información de la Decisión Marco (2005), se destacan tres principios distintivos: se trata de equipos, interconectados y que se utilizan para el tratamiento de datos. En paralelo, se definen otros tres conceptos esenciales en la materia de ciberdelincuencia:

- Datos informáticos: comprendidos como toda representación de hechos, informaciones o conceptos de una manera que permite su tratamiento por un sistema de información. En esta línea, se incluyen los programas que sirven para hacer que un sistema de información realice una función.

- Persona jurídica: entendida como toda entidad que el derecho le reconoce este estatuto. A excepción de aquellos Estados y otros organismos públicos que ejercen prerrogativas estatales y las organizaciones internacionales de derecho público.

- Falta de autorización: comprendido como todo acceso o intromisión ilegal a los datos o sistemas de información. Es decir, es el acceso no autorizado por el propietario o titular de otro tipo de derecho sobre el sistema o parte del mismo. O también, es el acceso que no se encuentra permitido en la legislación de un Estado.

Luego de las delimitaciones conceptuales, la Decisión Marco (2005) estipula las conductas que son consideradas merecedoras de reproche penal:

- El acceso ilegal a los sistemas de información: entendido como todo acceso intencionado y no autorizado a la totalidad o a parte de un sistema de información (artículo 2).

- Intromisión ilegal en los sistemas de información: definido como todo acto intencionado de obstaculizar o interrumpir de manera significativa el funcionamiento de un sistema de información. Más precisamente, todo acto realizado sin autorización, mediante la introducción, transmisión, daño, borrado, deterioro, alteración, supresión o inaccesibilidad de datos informáticos (artículo 3).

- Intromisión ilegal en los datos: comprende todo acto intencionado y cometido sin autorización con el objetivo de borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos informáticos contenidos en un sistema de información (artículo 4).

En cuanto al acceso ilegal a los sistemas de información, la Decisión Marco (2005) se puede considerar que se centra en la protección en aspectos estrechamente relacionados con la

intimidad o la inviolabilidad informática. Por lo que, su interpretación no se enfoca en proteger la integridad de los datos frente a posibles daños (Galán Muñoz, 2009). En otro orden de análisis, las conductas contempladas en el Convenio sobre la Ciberdelincuencia (2001) no son exactamente las mismas que se prevén en la Decisión Marco (2005). De allí que el debate doctrinario respecto de la compatibilidad entre ambos documentos.

Los Estados miembros de la Unión Europea que se adhirieron al Convenio quedan obligados a ajustar sus legislaciones penales conforme a sus directrices. Al mismo tiempo, deben realizar las modificaciones o adaptación de acuerdo a lo establecido en la Decisión Marco. En esta última se exige a los Estados que tres acciones en concreto sean reconocidas como conductas punibles penalmente. Sin embargo, se excluye la interceptación ilícita que si se encuentra estipulada en el Convenio.

Es posible que la exclusión de la interceptación ilícita entre las conductas tipificadas en la Decisión Marco en fundamentos basados en el bien jurídico protegido. Así, en la interceptación ilícita el bien jurídico protegido no son los datos o los sistemas de información propiamente dichos. Más bien, el bien jurídico protegido es el secreto de las comunicaciones o la intimidad que son valores ampliamente protegidos en las normativas constitucionales y penales de los Estados miembros (Fernández y Castro Fuertes (2009).

De acuerdo a Alonso, J. y González-Trevijano Sánchez (2004) “el derecho al secreto de las comunicaciones engloba tanto el secreto tradicional de la correspondencia […] como cualquier otra forma de comunicación […] especialmente el correo electrónico” (p. 137). Por consiguiente, las conductas evidentemente tipificadas en la Decisión Marco buscan proteger la integridad de los datos y los sistemas de información como bienes jurídicos nuevos que necesitan protección penal. En este marco, la interceptación ilícita excluida protege intereses que ya están regulados en otro tipo de ilícitos.

En este escenario, González Hurtado (2013) agrega que otra cuestión es evaluar si fue adecuado o no la exclusión de la interceptación ilícita contemplada en el Convenio. En primer lugar, pese a que el bien jurídico protegido pueda ser sustancialmente diferente, los métodos utilizados suelen ser los mismos. Además, parece deducirse de la regulación del Convenio que las cuatro acciones fueron concebidas como una serie de conductas que originalmente se pensaron dentro de disposiciones destinadas a otros tipos de delitos.

Es suma, el legislador internacional del Convenio intentó que las cuatro acciones tipificadas sean revestidas de autonomía normativa que les posible la separación de las figuras delictivas con las cuales, primitivamente, estaban asociadas. Tal autonomía normativa fue creada por la Decisión Marco para las tres primeras acciones mencionadas. A su vez, excluyó de esa misma autonomía a la interceptación ilícita. En consecuencia, mantuvo para esta modalidad la sujeción a la inviolabilidad de las comunicaciones según los diversos marcos legales.

Recapitulando, el primer artículo la Decisión Marco (2005) trata sobre la regulación de los daños informáticos. Así, entre el artículo segundo y cuarto se establecen las conductas que son consideradas merecedoras de reproche penal. Luego, se centra en otras cuestiones de tipo general. Así, el artículo quinto refiere al grado de participación en la acción típica: inducción, complicidad y tentativa. El artículo sexto refiere a las sanciones penales efectivas, proporcionales y disuasorias ante las infracciones mencionadas en los artículos anteriores. Además, en el artículo séptimo trata sobre las circunstancias agravantes respecto de las conductas punibles cuando se cometan en el marco de una organización delictiva. A continuación, en los artículos octavo y noveno se regulan los aspectos relacionados con las personas jurídicas. Primeramente, sobre la exigencia de responsabilidades por las infracciones señaladas entre los artículos segundo y quinto. En concreto, cuando sean cometidas por una persona, a título particular o como parte de un órgano de la persona jurídica

que ostente un cargo directivo en ella. En cuanto a las sanciones aplicables a las personas jurídicas se incluyen: multas de carácter penal o administrativo, exclusión del disfrute de ventajas o ayudas públicas, prohibición temporal o permanente del desempeño de actividades comerciales, vigilancia judicial, o medida judicial de liquidación.

Al margen de aquellos puntos relativos a la legislación penal, la Decisión Marco (2005) establece algunas cuestiones relativas a la competencia para enjuiciar los delitos anteriormente mencionados. En este orden, en el artículo décimo se instituye que los Estados deben hacer las modificaciones legislativas necesarias para juzgar a los autores de dichos delitos. Asimismo, aclara que se debe incluir a aquellos casos donde los efectos de las acciones delictivas se hayan producido en otros Estados.

De manera similar a lo consignado en el Convenio, la Decisión Marco insta a la necesidad de regular procedimientos análogos para el intercambio de información. Es decir, para el establecimiento de directrices comunes entre los Estados miembros de la Unión Europea. En perspectiva de las normas de protección de datos, se requiere que los países utilicen la red de puntos de contacto 24/7 que ya se encontraba en vigencia. También, en este artículo décimo primero se refiere a la designación de la administración que gestione aquella red en cada Estado miembro y su comunicación para que los demás estén al corriente de esta información.

Por último, el artículo décimo segundo establece plazos de aplicación de medidas necesarias para dar cumplimiento a la Decisión Marco. Es decir, manda a los Estados miembros a adoptar las medidas necesarias en derecho nacional antes del 16 de marzo de 2007. Por ello, deben remitir a la Secretaría General del Consejo y a la Comisión el texto de las disposiciones por las que incorporen a sus ordenamientos internos las obligaciones que la Decisión Marco les impone. A partir de esos datos, se elaboraría un informe a ser evaluado por el Consejo de la Unión Europea el 16 de septiembre de 2007.

Al respecto, González Hurtado (2013) analiza el proceso de incorporación de la Decisión Marco al derecho interno de los Estados miembros según los plazos de aplicación. De esta manera, se observa que no se llevó a cabo la evaluación del Consejo sobre la implementación de la normativa más allá de que la Comisión Europea presentó el informe previsto. Así, en el informe de la Comisión Europea (2008) se señala que para el 16 de marzo de 2007 solamente Suecia había cumplido en comunicar a la Comisión la forma de transposición a su legislación.

En consecuencia, se solicitó de nuevo a los Estados miembros el envío del texto informativo sobre las disposiciones nacionales de transposición de la Decisión Marco (2005). En respuesta, veinte Estados miembros comunicaron las reformas en sus ordenamientos penales. Mientras tanto, otros siete no cumplieron con la obligación de notificación impuesta. Por tanto, el informe concluye que la implementación de la normativa comunitaria en sus ordenamientos penales se encuentra en fase de transposición. Pese a la preocupación por los que no comunicaron el cumplimiento, se estima que el grado de aplicación de la normativa comunitaria es satisfactorio. Sobre todo, porque registraron notables progresos en los veinte Estados evaluados en el informe.

2.5.7. Comunicación acerca de dirigirse hacia una política general de lucha contra la ciberdelincuencia de 2007

La COM(2007)267 de la Comisión Europea al Parlamento Europeo, al Consejo y al Comité de las Regiones se inscribe en el proceso europeo de conformación de una política común contra la ciberdelincuencia. Así, a modo introductorio, recapitula los instrumentos internacionales elaborados hasta el año 2007. Y, en este caso puntual, la comunicación tiene como objetivo establecer una política general para mejorar la coordinación de la lucha contra la delincuencia informática a nivel internacional.

En el marco de la comunicación se proponen medidas para el abordaje de la ciberdelincuencia en perspectiva de mejorar la colaboración entre los diferentes actores de la Unión Europea. Ellas incluyen, el incremento de la cooperación operativa entre las autoridades policiales y judiciales. A su vez, proponen el aumento de la cooperación y coordinación políticas entre los Estados miembros. Así como también el fortalecimiento de la cooperación política y jurídica con países terceros. También, plantean el fomento del diálogo con la industria del sector, la sensibilización, la formación y la investigación en el ámbito de la ciberdelincuencia.

A los efectos, la Comisión Europea (2007) propone el establecimiento de una cooperación operativa reforzada entre las autoridades policiales y judiciales de los Estados miembros. En relación a ello, plantea la necesidad de aumentar el presupuesto destinado a la formación de estas autoridades en materia de delincuencia informática. Asimismo, insta al apoyo de la investigación en este campo. Al mismo tiempo, manda al sector público y privado a que se promuevan campañas de sensibilización sobre los costos y peligros de la ciberdelincuencia. Más precisamente, acciones de concientización dirigidas a toda la población y a los consumidores en particular.

En la comunican se busca el fomento de la cooperación internacional el abordaje de la ciberdelincuencia y se alienta a todos los Estados miembros y países terceros pertinentes a la adopción de medidas concretas para ratificar el Convenio sobre la Ciberdelincuencia (2001). En este sentido, se enfatiza en la particularidad de tratamiento que demandan los delitos que utilizan las redes informáticas para su comisión. Es por ello que, en el ámbito legislativo de la Unión Europea propone la realización de trabajos normativos específicos contra la usurpación de identidad, el fraude, el comercio ilícito y la lucha contra contenidos ilícitos en Internet.

En cuanto a las propuestas sobre los contenidos ilícitos González Hurtado (2013) destaca que es la más novedosa en algunos aspectos. Principalmente, propone como objetivo

la profundización del desarrollo de medidas para combatir este tipo delictivo. En especial, los contenidos ilícitos relacionados con el abuso sexual de menores y la apología del terrorismo. Además, se pide a los Estados miembros la asignación de recursos financieros suficientes para fortalecer el trabajo de los servicios policiales y judiciales.

También, en la comunicación se apoyan medidas en contra de los contenidos ilícitos que puedan incitar a los menores a comportamientos violentos. Por otra parte, se promueve el diálogo entre los Estados miembros y con países terceros sobre técnicas de lucha contra contenidos ilícitos y procedimientos para cerrar sitios web ilegales. Asimismo, se fomenta la elaboración de acuerdos en la Unión Europea entre autoridades públicas y operadores privados. Sobre todo, en consideración de los proveedores de servicios de internet, para la elaboración de los procedimientos de bloqueo y cierre de sitios ilegales en Internet.

2.5.8. Comunicación acerca de proteger Europa de ciberataques e interrupciones a gran escala de 2009

La COM(2009)149 es la Comunicación de proteger Europa de ciberataques e interrupciones a gran escala para aumentar la preparación, seguridad y resistencia. De esta manera, la Comisión Europea se dirige al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones respecto de la protección de infraestructuras críticas de información. La comunicación tiene como punto de partida los cálculos del Foro Económico Mundial (2008) sobre las probabilidades de que las infraestructuras críticas relativas a los sistemas informáticos sufrieran un fallo importante en un lapso de diez años.

De este modo, las estimaciones oscilaban entre el 10 % y el 20 %, con un coste potencial de hasta un billón de dólares. Además, se consideró que un ataque a los sistemas de información aparejaría una consecuencia dominó en otras infraestructuras como el agua, la energía y el

transporte. Para ilustrar mejor la gravedad de la situación, se mencionan los ciberataques en Estonia, Lituania y Georgia, como ejemplos de la necesidad de líneas de acción coordinadas.

Nuevamente, la Comisión Europea (2009) destaca en esta Comunicación que las actividades cotidianas, tanto privadas como profesionales, dependen cada vez más del desarrollo de los sistemas informáticos y las TIC. Por consiguiente, la protección de las infraestructuras críticas de información frente a la delincuencia informática a gran escala representa un desafío significativo para la sociedad y la economía europea. Además, se mencionan los principales retos que enfrentan dichas infraestructuras, como los virus informáticos, gusanos, spam y, en general, los programas con fines maliciosos.

En función de las problemáticas que expone la Comunicación propone un plan de acción destinado a reforzar la protección de las infraestructuras críticas de información. De esta forma, hace referencia a la necesidad de colaboración de los sectores público y privado. Por un lado, los Estados miembros como sector competente en la elaboración de las políticas en la materia para una protección eficaz. Y, por otra parte, el sector privado es responsable de su aplicación en tanto posee o controla un buen número de las infraestructuras críticas de información. Los ejes del plan de acción que propone la Comisión Europea (2009) son:

- Preparación y prevención: se solicita a los Estados miembros la definición de un nivel mínimo de capacidades y servicios para los Computer Emergency Response Team (CERT). Es decir, de los Equipos de Respuesta ante Emergencias de Informáticas a nivel nacional. Para ello, la comunicación insta a la colaboración con la Agencia Europea de Seguridad de las Redes y de la Información (European Network and Information Security Agency [ENISA]). En forma conjunta, se propone una asociación público-privada europea para mejorar la seguridad y la creación de un Foro europeo para facilitar el intercambio de información entre los Estados miembros.

- Detección y respuesta: se plantea la creación de un Sistema Europeo de Intercambio de Información y Alerta (European Information Sharing and Alert System [EISAS]) que llegue a los ciudadanos y las PYMEs.

- Mitigación y recuperación: se pide a los Estados miembros la elaboración de planes nacionales de contingencia y la organización de ejercicios de simulación de incidentes a gran escala de seguridad de las redes. Así como también manda a profundizar la cooperación entre los equipos CERT nacionales. Además, se enuncia el apoyo financiero para la realización de ejercicios paneuropeos que también pueden servir como plataforma operativa para la participación paneuropea en ejercicios internacionales.

- Cooperación internacional: se prevé la cooperación internacional en cuanto a la resistencia y estabilidad de Internet para la definición de prioridades, principios y directrices. Primero a escala europea, luego a nivel mundial.

- Criterios relativos a infraestructuras críticas europeas: se insta a su establecimiento el ámbito de los sistemas informáticos. Para que, de este modo, sea la base de la definición común, y sin contradecirla, se especifiquen las peculiaridades y los aspectos singulares a tener en consideración en las políticas de la Unión y de los Estados miembros.

2.5.9. Comunicación sobre la protección de infraestructuras críticas de información de 2011

La COM(2011)163 final, de 31 de marzo de 2011 es la trascendencia de la política europea que generó la comunicación del año 2009. En esta ocasión, la Comunicación de la Comisión Europea (2011) al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones fue relativa a la protección de infraestructuras críticas de información. En continuidad de la COM(2009)149, la Comunicación del año 2011 refiere,

puntualmente, a los logros y las próximas etapas (de dicha protección) hacia la ciberseguridad global.

De este modo, la Comisión Europea (2011) tiene como punto de partida el plan de acción de protección de infraestructuras críticas de la información según la Comunicación del 2009. Así, hace referencia al objetivo en el fortalecimiento de la seguridad y la resistencia de las infraestructuras de las TIC de acuerdo a los cinco ejes del plan de acción. También, a modo introductorio, menciona los pilares de la Agenda Digital para Europa de la COM(2010)245 final/2, de 26 de agosto de 2010.

En este orden, se enfatiza en las iniciativas de la comunicación del 2010 sobre seguridad en las tecnologías de la información que permitan la actuación inmediata de los organismos nacionales y europeos. Asimismo, se destacan las medidas en el ámbito penal y jurisdiccional para agilizar las infraestructuras críticas. Además, establece una clasificación de las amenazas que surgen en el marco de la delincuencia informática de acuerdo a los fines de su comisión:

- Fines de explotación: se refiere a las amenazas de espionaje económico y político o los robos de identidad. A su vez, es el caso de los ataques contra el sistema de comercio de derechos de emisión o contra los sistemas de los Estados.
- Fines de perturbación: relativa a la denegación de servicio distribuido, el spam o el corte de los medios de comunicación.
- Fines de destrucción física: prevé las posibilidades a futuro que se pueden generar a raíz de la omnipresencia creciente de las TIC en las infraestructuras críticas. Por ejemplo, inundaciones alterando los sistemas informáticos que regulan los recursos hidrográficos, catástrofes derivadas de la manipulación informática de sistemas que gestionan el correcto funcionamiento de las centrales eléctricas, entre otras conjeturas.

Por otro lado, la Comisión Europea (2011) recapitula brevemente los peligros a los que está expuesta la actual sociedad en la cultura de las TIC ante el carácter transnacional de la ciberdelincuencia:

> No son privativos de la Unión Europea, ni pueden ser resueltos por ella aisladamente. La omnipresencia de las TICs y de Internet permite que la comunicación, la coordinación y la cooperación entre los diferentes actores sea más eficaz, eficiente y económica, y da como resultado un dinámico ecosistema de innovación en todos los ámbitos de la vida. Pero el peligro puede surgir de cualquier lugar del mundo y, debido a la interconexión global, repercutir en cualquier lugar del mundo (p. 4).

En la misma línea que la comunicación de 2009, la Comisión Europea (2011) insiste en el abordaje de los desafíos de la protección de infraestructuras críticas de información. De este modo, efectúa una evaluación de los resultados que se logró con el plan de acción que se estableció en 2009. A su vez, la comunicación de 2011 expone las siguientes etapas estipuladas para la profundización de cada acción: preparación y prevención, detección y respuesta, mitigación y recuperación, cooperación internacional y criterios relativos a infraestructuras críticas europeas en el ámbito de los sistemas informáticos.

En cuanto a la preparación y prevención, se destacó que en 2009 se acordó que la ENISA y la comunidad de CERT de Europa colaboraron en el desarrollo y aprobación de un conjunto mínimo de capacidades y servicios de referencia que deben poseer los CERTs nacionales. Más precisamente, en los ámbitos del funcionamiento, la capacidad técnica, los mandatos y la cooperación, para poder funcionar de forma efectiva en perspectiva de la cooperación europea (Alamillo Domingo, 2009).

En el 2010 la ENISA y la comunidad de CERTs de Europa trabajaron de acuerdo al plan de acción, sobre todo en el ámbito de funcionamiento estableciendo directrices destinadas a los CERTs nacionales para que sean el factor principal de la preparación, la difusión de

información, la coordinación y la respuesta. Al respecto de los resultados, para el 2013 veinte Estados miembros desarrollaron CERT nacionales y casi todos los demás expresaron su voluntad de hacerlo

En lo relativo al objetivo de conformar un marco de gobernanza europea para la resistencia de las infraestructuras críticas se creó la Asociación Europea Público-Privada para la resiliencia (2009). Especialmente, su trabajo se refiere al fomento de la cooperación entre el sector público y el privado en el ámbito de seguridad. En el mismo año, se conformó el Foro Europeo para Estados Miembros como un espacio de debate e intercambio entre las autoridades públicas. Sobre todo, en materia de buenas prácticas, para compartir objetivos y prioridades políticas en materia de seguridad y resistencia de las infraestructuras informáticas y de telecomunicaciones.

En el mismo sentido se delinearon los objetivos para los años siguientes para la instauración de CERTs nacionales en los Estados que aún estaban pendientes. El fin último es proseguir esta labor hasta completar la totalidad de los miembros de la Unión Europea. Una vez alcanzado, se prevé someter a consideración la conveniencia de ampliar sus capacidades hasta convertirlos en el eje del Sistema Europeo de Intercambio de Información y Alerta (EISAS) al servicio de los ciudadanos y las PYMEs. Igualmente, se prevé que se continúe fomentando la labor de la Asociación Europea Público-Privada para la resiliencia ante nuevos ataques basados en instrumentos innovadores (González Hurtado, 2013).

Al respecto del segundo eje del plan de acción de la comunicación de 2009, detección y respuesta, la comunicación del 2011 refiere a la labor que la ENISA proyectó para el 2013. Así, se destaca que la ENISA elaboró una hoja de ruta para la creación del Sistema Europeo de Intercambio de Información y Alerta (EISAS). De esta forma, las próximas etapas previstas se centran en el apoyo a los Estados miembros en la implementación de la hoja de ruta del EISAS. El objetivo principal se refiere al desarrollo de los servicios básicos que los Estados miembros

de la Unión Europea utilizarán para crear su Sistema de Intercambio de Información y Alerta a partir de sus CERT nacionales. A través de ello, la ENISA debe proceder con el desarrollo de los servicios de interoperabilidad que faciliten a cada Sistema de Intercambio de Información nacional.

En el tercer eje del plan de acción de la comunicación de 2009 se hizo referencia a la mitigación y recuperación. Más precisamente, para la elaboración de programas nacionales de contingencia y organización de ejercicios de respuesta ante incidentes a gran escala de seguridad de las redes. Además, de acuerdo a este tercer eje, se desarrollaron planes de recuperación en caso de catástrofes antes de finalizar el año 2010. Asimismo, la ENISA realizó una guía de buenas prácticas para ejercicios nacionales y recomendaciones "en materia de política de desarrollo de estrategias nacionales con el fin de respaldar las actividades de los Estados miembros, que deben intensificarse" (Comisión Europea, 2011, p. 6).

También, entre los avances logrados en este eje, se destaca que la ENISA organizó eventos a nivel internacional con los Estados miembros a través de los CERT nacionales. Al mismo tiempo, dedicó esfuerzos al fortalecimiento de la cooperación entre los CERT nacionales de los diferentes Estados de la Unión Europea. A futuro, se proyecta que se profundice la labor de apoyo de la ENISA a los Estados miembros en planes nacionales de contingencia, ejercicios periódicos de respuesta y de recuperación en caso de catástrofe. El fin último es el establecimiento de una vía hacia una cooperación paneuropea más estrecha.

Acerca del cuarto eje del plan de acción de la comunicación de 2009, la Cooperación internacional, se destacó la labor llevada adelante por el Foro Europeo para Estados Miembros. De este modo, la comunicación de 2011 se refiere al debate y elaboración de principios y directrices europeos sobre resistencia y estabilidad de Internet. En función de estos principios, la Comisión Europea (2011) asumió el rol de elevar a debate con las partes interesadas más relevantes. Especialmente, con el sector privado a través de la Asociación público-privada

europea de resistencia. Así como con socios internacionales más importantes, tanto en términos bilaterales, como con los Estados Unidos, y de forma multilateral, con el G8, la OCDE, Meridian y la UIT.

En suma, el horizonte es que a partir de 2012 los principios y orientaciones europeos sobre resistencia y estabilidad de Internet se conformen como un marco común de compromiso colectivo internacional a largo plazo. Al mismo tiempo, se prevé continuar con la celebración de ciberejercicios de seguridad informática de las telecomunicaciones a nivel internacional. Primordialmente con regiones o países que reconozcan problemas análogos en la materia para compartir estrategias y actividades.

El último eje de acción que se proyectó en la comunicación de 2009 fue el establecimiento de criterios relativos a infraestructuras críticas europeas. En relación a ello, la comunicación de 2011 señala los debates técnicos en el Foro Europeo para Estados Miembros sobre los criterios sectoriales específicos de las TIC. A partir de este trabajo, se concluyó en el planteamiento de la fase inicial de un proyecto de criterios aplicables a las comunicaciones (móviles y fijas) e Internet. De manera semejante, se planificó la celebración de consultas con el sector privado sobre este proyecto de criterios para el sector de las TIC.

Al final, la comunicación de 2011 concluye en un hecho que se confirma en los distintos instrumentos internacionales en la materia: la necesidad de un abordaje transnacional. En palabras de la Comisión Europea (2011) “la experiencia demuestra que, a la hora de abordar cuestiones de seguridad y resistencia, un enfoque puramente nacional o regional no basta” (p. 6). En función de lo cual, se afirma que en el escenario europeo es esencial que se continúe dedicando esfuerzos para construir una estrategia coherente y cooperativa de los Estados miembros. En cuanto a la protección de los sistemas informáticos y de comunicación a largo plazo se subraya el rol de la ENISA como agencia central de apoyo a los Estados miembros, las instituciones de la Unión Europea y el sector privado.

Como puede advertirse, el proceso evolutivo en materia de seguridad informática que emprendió la Unión Europea resulta sumamente amplio. En especial, por su carácter abarcativo, que comprende a la seguridad informática desde el ámbito de la delincuencia informática y desde una perspectiva global (legislación, infraestructuras, organismos, etc.). "No hablamos, por tanto, sólo de medidas legislativas puntuales, sino de una verdadera política de seguridad informática y de las telecomunicaciones acorde a las necesidades y características de la sociedad de la información actual" (González Hurtado, 2013, p. 130).

2.5.10. Comunicación sobre la represión del delito en la era digital y la creación de un centro europeo de ciberdelincuencia de 2012

En el proceso de abordaje de la ciberdelincuencia de la Comisión Europea, la comunicación de 2012 sigue las líneas trazadas por la comunicación de 2011. Así, se emite la COM(2012)140 final, de 28 de marzo de 201, al Consejo y al Parlamento Europeo sobre la represión del delito en la era digital. En esta oportunidad, la comunicación presenta como eje central a la creación de un centro europeo de ciberdelincuencia. Además, a diferencia de las comunicaciones anteriores que lo abordaban desde una perspectiva general, esta comunicación se centra concretamente en el ámbito de la delincuencia informática.

A modo introductorio, se señala que los sistemas informáticos e Internet son un espacio abierto sin límites nacionales ni una estructura de gobernanza. Así, por un lado, se presenta a este fenómeno como una parte indispensable de la sociedad actual en todos los aspectos. A su vez, se menciona el multimillonario coste que la delincuencia informática supone para la sociedad actual. A partir de este escenario, la Comisión Europea (2012) expone algunas de las iniciativas que desarrolló en el ámbito penal para contrarrestar los efectos que produce la diversidad legislativa de los Estados miembros en este ámbito.

A continuación, la comunicación de 2012 destaca las Decisiones Marco del 2003 y 2005. La primera refiere a la lucha contra el abuso de menores y la pornografía infantil en el marco de los sistemas informáticos y las redes. La segunda enfatiza la delincuencia informática vinculada con el fraude informático, la falsificación electrónica, la intromisión ilícita y los daños informáticos. Luego, se considera que la Decisión Marco de 2003 se sustituyó por una Directiva de 2011 que mejora y amplía la regulación mencionada.

En conjunto con estos instrumentos legislativos, se posiciona el trabajo que la Europol desempeña en relación con la delincuencia informática. Desde otro ámbito, menciona el rol de la cooperación internacional a través del Convenio sobre la Ciberdelincuencia (2001). Al respecto, se puntualiza en la necesidad de que más Estados se adhieran al mismo. Sobre todo, en perspectiva de estrechar las relaciones en esta materia fuera del entorno de la Unión Europea.

En este marco descrito, la Comisión Europea (2012) propone la creación de un Centro Europeo de Ciberdelincuencia. En el proceso de desarrollo de la Unión Europea, este Centro otorga contenido a la Plataforma Europea de Cibercrimen de 2008 y a la acción prevista en la Agenda Digital Europea de 2010. Es así que, se proyecta que el Centro se enfoque en tres campos de actuación principales:

- Los ciberdelitos cometidos por grupos de la delincuencia organizada, especialmente los que generan extensos réditos ilegales mediante el fraude en línea.
- Los ciberdelitos que provocan daños graves a sus víctimas, como la explotación sexual de menores en línea.
- Los ciberdelitos (incluidos los ciberataques) que afectan a infraestructuras y sistemas de información esenciales de la Unión Europea.

Además, se prevé que el Centro desempeñe como funciones principales:

- Servir de punto central de información sobre la delincuencia en Europa: con la función de reunir toda la información vinculada con la delincuencia informática en los Estados

miembros y del ámbito internacional. Para ello, se considera la utilización de todas las fuentes disponibles, tanto gubernamentales como privadas, en perspectiva de recolectar los distintos datos policiales existentes.

- Aunar el conocimiento sobre ciberdelincuencia europea para contribuir a la capacitación de los Estados miembros. De acuerdo a esta función, debe concentrar los conocimientos especializados en delincuencia informática para poder asistir a los Estados miembros y a sus funcionarios judiciales o policiales en labores de formación. Al mismo tiempo, implica que debe elaborar manuales de buenas prácticas y colaborar en el desarrollo de la cooperación internacional en el abordaje de la ciberdelincuencia.

- Prestar apoyo a los Estados miembros en investigaciones de ciberdelincuencia. Así, debe asumir como función el fomento de la creación de equipos conjuntos de investigación e intercambio de información para facilitar las investigaciones nacionales.

- Ser la voz colectiva de los investigadores de ciberdelincuencia europeos ante los organismos de orden público y el estamento judicial. En esta función se espera a futuro que el Centro logre funcionar como punto de reunión de los investigadores europeos en el campo de la delincuencia informática. Más aún, se planifica que el Centro se convierta en un foro de intercambio de profesionales de diversos ámbitos (judicial, policial, industrial, etc.).

A partir de esta comunicación, se materializó la creación del Centro Europeo de Ciberdelincuencia. Más precisamente, se encuentra operativo desde el año 2013 como parte de la estructura de la Europol. Asimismo, el Centro entabla relaciones con otros actores interesados: Eurojust, la Escuela de Policía Europea (CEPOL Collège Européen de Police), los Estados miembros representados por el Grupo Especial de Ciberdelincuencia de la Unión Europea, la ENISA y la Comisión (González Hurtado, 2013).

CAPÍTULO III.

LOS DELITOS INFORMÁTICOS EN PERSPECTIVA REGIONAL

En el capítulo anterior se puso en evidencia que la necesidad abordaje de los delitos informáticos provocó profundos cambios en el ámbito de la asistencia judicial internacional. Sobre todo, debido a la ubicuidad de la criminalidad informática que a menudo produce perplejidad a las jurisdicciones locales por la dificultad de determinar nociones que antes eran consideradas básicas. La naturaleza peculiar de los delitos informáticos torna sumamente compleja la investigación para determinar cuestiones como el lugar de ocurrencia del delito o las normas procedimentales para la obtención de la prueba.

En el escenario de la Sociedad de la Información o el mundo globalizado se introdujeron nuevos actores en la investigación del delito informático. Así, confluyen tanto actores públicos como privados debido a que las características de este tipo de ilícito demandan la mutua colaboración. Por un lado, el sector privado que involucra a los que prestan servicios relacionados con internet; por otro, el sector público que implica a los Estados a través de sus órganos judiciales y de seguridad, tanto a nivel nacional como internacional porque los delitos informáticos trascienden fronteras y jurisdicciones.

Tal diversidad de actores que intervienen en la investigación de los delitos informáticos rompió el esquema clásico de la asistencia judicial internacional, basada en cooperación tradicional entre Estados Nacionales y/o organismos internacionales y/o regionales. Así, la investigación de la ciberdelincuencia demandó colaboraciones e intercambios de información entre órganos judiciales, sin distinción de nacionalidad, y las empresas que prestan servicios en internet y las proveedoras de servicios de internet. En este marco, la asistencia internacional se rige a partir de la paulatina elaboración de manuales de buenas prácticas y guías de acción para fuerzas de la ley (Deluca y Del Carril, 2017).

De este modo, el establecimiento de directrices implica propuestas de las compañías de internet y la interpretación de las normas locales que las obligan. Inclusive, reciben la influencia de las relaciones interpersonales que generan vínculos de confianza entre las empresas y las instituciones públicas. De esta manera, el tratamiento del fenómeno en constante evolución demanda un desempeño fundamental a los organismos internacionales para generar prácticas homogéneas que vinculen a los Estados (Schiff Berman, 2005).

Al mismo tiempo, los organismos internacionales pueden proporcionar a los particulares un marco normativo que les ofrezca previsibilidad y que al mismo tiempo los proteja de eventuales consecuencias jurídicas (incluso penales) al enfrentarse a una multitud de sistemas jurídicos diferentes. En este orden, los esfuerzos para alcanzar la armonización legislativa se pueden ejemplificar exitosamente con el Convenio sobre la Ciberdelincuencia (2001). Cabe agregar que, aunque se trata de un instrumento acordado en el ámbito europeo tiene la particularidad de haber sido abierta a la firma de cualquier país del mundo (Díaz Gómez, 2010).

En otros órdenes internacionales como ONU se continúan dedicando esfuerzos para la elaboración de convenios similares al de Budapest. Por ejemplo, se aprobó un capítulo relativo al cibercrimen en el marco de la Oficina de las Naciones Unidas contra la Droga y el Crimen para consensuar la celebración de un convenio de estas características. En el ámbito interamericano, la Organización de los Estados Americanos (OEA) aprobó la Estrategia Interamericana Integral para Combatir las Amenazas a la Seguridad Cibernética (2004). Todas estas medidas son parte de un modelo supranacional que es acertado teniendo en cuenta que el problema de la cibercriminalidad supera los límites territoriales.

3.1. Organización de los Estados Americanos

El auge de las tecnologías trajo aparejado innumerables avances para la humanidad. A su vez, implicó una serie de desafíos para las autoridades, legisladores e investigadores en las Américas. No debe sorprender que en este contexto los delitos informáticos se convirtieron en un fenómeno cada vez más demandante para su persecución y sanción a nivel regional (OEA, 2016). En marzo de 1999 los Ministros de Justicia o Ministros o Procuradores Generales de las Américas (REMJA) recomendaron establecer un grupo de expertos intergubernamentales sobre delito cibernético con el objeto de:

- Realizar un diagnóstico de la actividad delictiva relacionada a las computadoras y la información en los Estados miembros.
- Hacer un diagnóstico de la legislación, las políticas y las prácticas nacionales sobre delito cibernético.
- Identificar las entidades nacionales e internacionales que tienen experiencia en la materia.
- Identificar mecanismos de cooperación dentro del sistema interamericano para combatir el delito cibernético.

3.1.1. I y II Reunión de Expertos Gubernamentales en Delito Cibernético

En perspectiva de las metas fijadas por REMJA, se convocó a la I Reunión de Expertos Gubernamentales en Delito Cibernético en la Sede de la OEA (1999). Para lograr el cumplimiento de sus objetivos el grupo de expertos elaboró un cuestionario a través del cual solicitó información a los Estados miembros sobre su experiencia en la materia. De esta manera, se indagaba acerca de los tipos de delito cibernético, leyes sustantivas, principios de jurisdicción y de extradición que los rigen. También, se preguntaba sobre las leyes que rigen la conservación y recolección de pruebas en casos de delito cibernético. Además, se examinaba

la existencia de programas especializados de capacitación o entidades y/o expertos en cumplimiento de las leyes para combatir el delito cibernético.

Consecutivamente, se celebró la II Reunión de Expertos Gubernamentales sobre Delito Cibernético (1999). En esta oportunidad, el objetivo fue el análisis de los datos recolectados según las respuestas de los gobiernos de los Estados miembros al cuestionario de la Primera Reunión. Asimismo, se hizo alusión a los mecanismos de cooperación en el sistema interamericano sobre delito cibernético. También fue parte de la agenda, una exposición realizada por expertos convocados de distintos organismos públicos y privados de la esfera de la informática.

Solamente once Estados miembro respondieron el cuestionario de la Primera Reunión de Expertos: México, Estados Unidos, Ecuador, Brasil, El Salvador, Costa Rica, Perú, Argentina, Trinidad y Tobago, Panamá y Venezuela. Aunque el número de respuestas fue limitado, el grupo de expertos consideró que era suficientemente representativo de la situación general de las Américas. A partir de los datos recolectados, se realizó un informe con recomendaciones para los Estados miembros.

El informe revela que siete Estados miembros no reportaron perjuicios considerables como resultado del delito cibernético. Las respuestas de estos países dan cuenta de que el delito cibernético se percibe como un fenómeno todavía poco común y que, frecuentemente, no se sancionan leyes específicas. Sin embargo, en algunos Estados miembros se penalizan conductas delictivas cometidas con la utilización de tecnologías de la información. Por ejemplo, el fraude, la evasión tributaria, la difamación o la distribución de pornografía infantil. Ante este panorama, se consideró relevante el desarrollo, adecuación y armonización de la legislación, los procedimientos y las instituciones para abordar el abuso y el uso erróneo de las computadoras en los Estados miembros.

Otro aspecto que se consideró en el informe fue la legislación sobre recolección de pruebas, con especial énfasis en para la investigación de delitos cibernéticos relativos a la facultad para rastrear, recoger, preservar y divulgar información sobre tráfico de comunicaciones electrónicas y datos informativos. Nueve Estados miembros respondieron que: "sus legislaciones sí permiten el aseguramiento de materiales tangibles de conformidad con procedimientos, así como obligar a los proveedores de acceso a la Internet y compañías de telecomunicaciones que presenten información sobre suscriptores y sobre cobranzas" (II Reunión de Expertos Gubernamentales sobre Delito Cibernético, 1999, p. 3).

Los Estados miembro afirmaron la existencia de legislaciones internas que garantizaban la recolección de pruebas para la investigación de delitos cibernéticos. Cabe agregar que en algunos casos no se les permitía a los investigadores que tomen otras medidas pertinentes para investigar estos ilícitos. En este orden, se referían a medidas para obtener información de fuente y destino sobre comunicaciones en forma simultánea con la transmisión de ellas. Por lo cual, se trataba de un procedimiento que puede ser necesario para el seguimiento de una intromisión cibernética.

Una de las mayores dificultades que la II Reunión tuvo en consideración fue la falta de entidades especializadas en el área y la carencia de capacitación correspondiente. En muchos casos, el delito cibernético es investigado por unidades que no están especializadas en delitos cibernéticos, como ser entidades de delincuencia organizada o narcotráfico. De esta manera, se destacó que esta falencia puede traer serios perjuicios en las investigaciones a nivel nacional e internacional sobre este tipo de delitos; y se estimó como una prioridad en este campo a ser desarrollada mediante mecanismos adecuados de capacitación.

En base a las respuestas al cuestionario se concluyó que muy pocos Estados miembro enfrentaron problemas relativos con la naturaleza transnacional del delito cibernético. Tampoco brindaron o recibieron solicitudes de ayuda internacional en la materia. Sin embargo,

es usual que los países de las Américas rastreen un delito cibernético a través de redes de computadoras ubicadas en múltiples países no vinculados con el lugar del delincuente o la víctima del delito. Por lo tanto, se estima que la capacidad de solicitar y proporcionar ayuda internacional es esencial y debe ser examinada detalladamente.

El diagnóstico sostiene que quedan dudas sobre la regulación de la jurisdicción, extradición y cooperación internacional:

> De los resultados de la encuesta no se desprende con claridad si los temas relativos a jurisdicción, extradición y cooperación internacional están regidos adecuadamente por las leyes de aplicación específica o general de los Estados miembros y los acuerdos multilaterales y bilaterales existentes (II Reunión de Expertos Gubernamentales sobre Delito Cibernético, 1999, p. 3).

Por último, se prevé el fenómeno del delito cibernético a futuro debido a que los resultados de la encuesta de 1999 manifiestan que no aún se percibían a nivel regional los daños causados hasta ese entonces. Las presentaciones realizadas por representantes de diversas entidades internacionales, gobiernos, entidades del sector privado y organizaciones de seguridad informática, destacaron la expansión del delito cibernético. Por consiguiente, se afirmó que era crucial asegurar que los Estados miembros estén preparados para investigar y procesar el delito cibernético cuando ocurra en sus jurisdicciones.

Luego del apartado del diagnóstico, el informe de la II Reunión refiere a la identificación de entidades nacionales con conocimientos especializados pertinentes. De este modo, el grupo de expertos identificó las siguientes entidades internacionales en materia de delito cibernético: el Consejo de Europa, el Grupo de los Ocho, la Unión Europea, la OCDE, la ONU y la Organización Internacional de Policía Criminal (INTERPOL). Además, menciona la existencia de entidades académicas y del sector privado que tienen conocimientos

especializados. Por ejemplo, las empresas de telecomunicaciones y “equipos de respuesta” a emergencias informáticas de la Universidad Carnegie-Mellon de los Estados Unidos.

En el siguiente punto, el informe identifica los mecanismos de cooperación en el sistema interamericano en la lucha contra el delito cibernético. En especial, menciona los tratados de asistencia jurídica mutua (bilaterales y multilaterales), la INTERPOL, las cartas rogatorias y los mecanismos informales de cooperación. Al mismo tiempo, señala que algunos Estados miembros se sumaron o expresaron la voluntad de formar parte del Grupo Punto de Contacto de 24 horas/7 días.

A continuación, en el informe de la II Reunión de Expertos, se establecen diez recomendaciones. De este modo, se reconoce la amenaza global que plantea el delito cibernético y la necesidad de una respuesta adecuada y rápida por parte de las autoridades nacionales competentes. Ellas fueron las siguientes:

- Instar a los Estados miembros a que establezcan una entidad o entidades públicas con la autoridad y función específica para llevar adelante la investigación y persecución del delito cibernético.
- Instar a los Estados que no tenían legislación sobre delitos cibernéticos a que emprendan acciones en este sentido.
- Solicitar a los Estados miembros que realicen todos los esfuerzos necesarios para armonizar sus legislaciones en materia de delito cibernético, a fin de facilitar la cooperación internacional para la preservación y combate de estas actividades ilícitas.
- Instar a los Estados miembros a que identifiquen sus necesidades de capacitación en materia de delito cibernético, propiciándose esquemas de cooperación bilateral, regional y multilateral en este campo.
- Propiciar la formulación de lineamientos generales para orientar los esfuerzos legislativos en materia de delito cibernético.

- Considerar diversas medidas incluyendo el establecimiento de un Fondo Específico Voluntario, para apoyar el desarrollo de la cooperación en el Hemisferio sobre la materia.
- Propiciar entre los Estados miembros el intercambio de información en materia de delito cibernético.
- Apoyar la difusión de información sobre las actividades desarrolladas en el ámbito de la OEA en esta materia, incluyendo la página Web sobre el particular.
- Instar a los Estados miembros a que consideren la posibilidad de sumarse a mecanismos de cooperación o intercambio de información ya existentes, tales como el "Grupo de contracto de 24 horas/7 días" a fin de iniciar o recibir información.
- Instar a los Estados miembros a que tomen medidas para sensibilizar al público, incluyendo a los usuarios del sistema educativo, del sistema legal y administración de justicia sobre la necesidad de prevenir y combatir el delito cibernético (II Reunión de Expertos Gubernamentales sobre Delito Cibernético, 1999).

3.1.2. III Reunión de Expertos Gubernamentales sobre Delito Cibernético

Tras cuatro años de las primeras deliberaciones se realizó la III Reunión de Expertos Gubernamentales sobre Delito Cibernético, en la Sede de la OEA (2003). En aquella ocasión se acordaron numerosas recomendaciones con el objetivo de impulsar el progreso en áreas clave para mejorar y consolidar la cooperación en toda la región. Primeramente, se destacó la importancia de que los Estados establezcan entidades especializadas en la investigación y persecución de delitos cibernéticos. En este orden, se instó a la asignación de los recursos humanos, financieros y técnicos necesarios para desempeñar sus funciones de manera eficaz, eficiente y oportuna. Además, se recomendó que los Estados revisen sus marcos legales para confirmar que sean aplicables a la investigación de los delitos cibernéticos. En este orden, se sugirió que los Estados adopten la legislación necesaria para definir claramente los distintos

tipos de delitos cibernéticos. Lo mismo en lo relativo al establecimiento de procedimientos que garanticen la recolección y protección segura de indicios y/o pruebas electrónicas. Para facilitar este proceso, se propuso la organización de reuniones técnicas dentro del marco de la OEA. De esta manera, se plantea la asistencia para la redacción de legislación, la armonización de las legislaciones nacionales y la promoción de la cooperación efectiva a nivel hemisférico.

Otra recomendación importante fue que la Secretaría General de la OEA cree y mantenga actualizado un directorio que incluya los puntos de contacto de cada uno de los Estados miembros. Se propuso también la existencia de un directorio referente a las autoridades responsables de la investigación y persecución del delito cibernético. Asimismo, se instó a los Estados a unirse, lo antes posible, a la "Red de Emergencia de 24 horas/7 días", que permite una respuesta rápida ante incidentes en la materia.

La recomendación subrayó la necesidad de seguir desarrollando un sistema integral de información sobre los avances en la lucha contra el delito cibernético y sugirió que se incluya tanto una parte pública como una de acceso restringido para las autoridades competentes. Igualmente previó que se recopile las legislaciones de los Estados miembro en la materia e identifique las áreas temáticas comunes entre estas y se publique en el sitio web de la OEA y recomendó que los Estados incorporen formación específica en delitos cibernéticos y manejo de pruebas electrónicas en los programas de capacitación para jueces, fiscales y cuerpos policiales. Para lo cual, se solicita la cooperación técnica mutua entre los Estados Miembros y los Observadores Permanentes de la OEA. Por último, se recomendó seguir dedicando esfuerzos al fortalecimiento del intercambio de información y la cooperación con otras organizaciones internacionales. Por ejemplo, las Naciones Unidas, el Consejo de Europa, la Unión Europea, el Foro de Cooperación Económica del Pacífico Asiático (APEC), la OCDE, el G-8 y el Commonwealth. Siendo así, el objetivo es que los Estados Miembros de la OEA puedan beneficiarse de los avances en estos ámbitos. Para cerrar esta serie de recomendaciones,

se acordó que el Grupo de Expertos se reúna al menos una vez al año para seguir coordinando esfuerzos en el combate del delito cibernético.

En el mismo año de la III Reunión del Grupo de Expertos Gubernamentales (2003) se realizó la Conferencia Especial sobre Seguridad en el seno de la OEA. El resultado fue la adopción de la Declaración sobre seguridad en las Américas (2003) que amplía la definición tradicional de defensa de la seguridad de los Estados. De esta manera, adquiere un enfoque multidimensional, que incluye aspectos políticos, económicos, sociales, de salud y ambientales. A su vez, el concepto de seguridad se amplía con la incorporación de nuevas amenazas, preocupaciones y desafíos de diversa índole (Chillier y Freeman, 2005).

En este escenario, las problemáticas que ponen en peligro la seguridad se caracterizan por su naturaleza transnacional que demandan la cooperación de todos los Estados miembros. Entre ellas, relativa a la materia de delitos informáticos, se mencionan los ataques a la seguridad cibernética. A raíz de ello, se celebró el compromiso de la implementación de medidas preventivas efectivas que permitan anticipar, gestionar y responder a los ataques cibernéticos. En ese orden de ideas se instó al combate "contra las amenazas cibernéticas y la delincuencia cibernética, tipificando los ataques contra el espacio cibernético, protegiendo la infraestructura crítica y asegurando las redes de los sistemas" (ONU, 2003, párr. 26).

Es importante destacar que la Declaración sobre seguridad en las Américas (2003) enmarca la cuestión de la seguridad cibernética en los mecanismos de cooperación dentro del sistema interamericano. En dicho contexto se mencionan las recomendaciones elaboradas conjuntamente por los expertos de los Estados Miembros y el Grupo de Expertos Gubernamentales de la REMJA en Materia de Delito Cibernético. Luego, se destaca el trabajo de la Comisión Interamericana contra el Terrorismo (CICTE), la Comisión Interamericana de Telecomunicaciones (CITEL) y otros órganos apropiados en la materia.

Por lo tanto, se tiene en cuenta como antecedente fundamental los trabajos realizados en este ámbito en perspectiva de implementar una estrategia integral en el marco de la OEA. En este escenario regional se generaron distintas instancias de concertación que reunió la participación de los gobiernos, del sector privado y de la sociedad civil. Todo ello, con el objeto de la identificación de las necesidades nacionales de seguridad cibernética y la formulación de políticas específicas. "La transnacionalidad, el terrorismo, la tecnología, Internet no solo han eventualmente signado la agenda internacional de estos tiempos, sino que resumen en materia de ciberseguridad una característica sustancial de la sociedad internacional" (Ibarra y Nieves, 2016, párr. 1).

De lo expresado surge claramente que la Declaración sobre seguridad en las Américas (2003) fue el primer instrumento interamericano que reafirmó la necesidad de desarrollar una cultura de seguridad cibernética supranacional en la región. En este compromiso internacional se insta a la adopción de medidas de prevención de ataques, combate contra las amenazas cibernéticas y su tipificación jurisdiccional. Al año siguiente, estos esfuerzos internacionales se materializaron en la resolución de "Adopción de una Estrategia Interamericana Integral para combatir las amenazas a la Seguridad Cibernética: un enfoque multidimensional y multidisciplinario para la creación de una cultura de seguridad cibernética".

3.1.3. Estrategia Interamericana Integral de Seguridad Cibernética

La Estrategia Interamericana Integral de Seguridad Cibernética (2004) amplió la protección de seguridad sobre redes y sistemas de información ante las amenazas de ataques maliciosos o delictivos. Una vez más se afirma la necesidad de llevar adelante un esfuerzo coordinado en la lucha contra las amenazas cibernéticas en las Américas. Para ello, la resolución se presenta como un marco de fortalecimiento de la capacidad de los Estados

Miembros en la protección de las infraestructuras críticas, la economía y las personas frente a la delincuencia cibernética.

La resolución conforma, de tal modo, un espacio que propicia el flujo de información y la protección de la infraestructura de las TIC. También se presenta como una herramienta que fortalece la capacidad para gestionar las amenazas cibernéticas y la resiliencia individual y colectiva frente a este fenómeno. Así, la resolución se manifiesta como parte de los compromisos de la OEA a lo largo de los años que subrayan la responsabilidad internacional en la promoción de la seguridad cibernética y la lucha contra la delincuencia informática (Observatorio de la ciberseguridad en América Latina y el Caribe, 2016).

Como puede advertirse, la Estrategia Interamericana Integral de Seguridad Cibernética (2004) insta al trabajo conjunto de los Estados miembros con las entidades de la OEA. Es decir, el CICTE, la CITEL y el Grupo de Expertos Gubernamentales en materia de Delito Cibernético de las Reuniones de REMJA. En este marco, se encuentran comprometidos en el fomento de una cultura de seguridad cibernética que disuade el uso indebido de internet y de los sistemas de información y la promoción del desarrollo de redes de información que sean de confianza y fiables.

La resolución reconoce la necesidad de mejorar la seguridad de las redes y sistemas de información (internet) con el objetivo de enfrentar vulnerabilidades y proteger a los usuarios, sobre todo, en el ámbito de la seguridad nacional y las infraestructuras críticas, contra las amenazas en el espacio cibernético con intenciones criminales. Para abordar estos retos, se destaca la importancia de establecer una red interamericana de alerta y vigilancia, que permita la rápida distribución de información, respuesta y recuperación ante amenazas cibernéticas. Más aún, se enfatiza en la urgencia de desarrollar redes y sistemas de internet fiables para fomentar la confianza del usuario en estas infraestructuras (Temperini, 2014).

Es más, se reitera, como en los antecedentes en la materia, la importancia de diseñar una estrategia global que proteja la infraestructura de información, que tenga un enfoque integral, internacional y multidisciplinario. Desde esta perspectiva, se consideran las resoluciones 55/63 y 56/ 121 de la Asamblea General de la ONU que abordan la lucha contra el uso delictivo de la tecnología de la información. También, se mencionan especialmente las resoluciones 57/239 y 58/199 que destacan la necesidad de fomentar una cultura mundial de seguridad cibernética y la protección de las infraestructuras de información esenciales.

En este escenario, la Asamblea General de la ONU resolvió la aprobación del proyecto de Estrategia Interamericana Integral de Seguridad Cibernética (2004) e instó a los Estados Miembros a ponerla en práctica. También les solicitó que establecieran Equipos de Respuesta a Incidentes de Seguridad en Computadoras (CSIRT) para mejorar la capacidad de respuesta ante ciberataques. Particularmente, la resolución subrayó la importancia de garantizar que los sistemas de información de internet sean seguros en todo el hemisferio y solicitó al Consejo Permanente, a través de la Comisión de Seguridad Hemisférica, que continúe tratando este tema y facilite la coordinación para implementar la Estrategia. También exhortó a los Estados Miembros y entidades de la OEA a la coordinación de esfuerzos para el fortalecimiento de la seguridad cibernética en la región, y pidió a las Secretarías del CICTE y la CITEL y al Grupo de Expertos Gubernamentales que apoyen a los Estados Miembros en la implementación de la Estrategia. La resolución instó a la presentación de un informe con el Consejo Permanente por medio de la Comisión de Seguridad Hemisférica sobre el progreso de la observancia de esta resolución antes del trigésimo quinto período ordinario de sesiones de la Asamblea General.

En dicho contexto se respaldó la realización de la II Reunión de Practicantes Gubernamentales en Materia de Seguridad Cibernética en el marco del CICTE con la finalidad de dar seguimiento a las recomendaciones sobre el Establecimiento de la Red Interamericana de Alerta y Vigilancia. Además, esta reunión se debería llevar a cabo utilizando los recursos

asignados en el programa-presupuesto de la Organización, y otros recursos adicionales. Se puso a su disposición el apoyo administrativo y técnico de la Secretaría General y la Secretaría del CICTE.

En la resolución se pidió a los Estados Miembros la observación de las recomendaciones de la reunión inicial y la quinta reunión del Grupo de Expertos Gubernamentales en Materia de Delito Cibernético de la REMJA. Tales medidas se estimaron fundamentales en el establecimiento de un marco legal que proteja los sistemas de información, evite el uso de computadoras para actividades ilícitas y sancione el delito. Por último, se solicitó al Consejo Permanente que informe a la Asamblea General en su trigésimo quinto período ordinario de sesiones sobre los avances del cumplimiento de esta resolución.

En la resolución sobre la Estrategia Integral de Seguridad Cibernética (2004) se destaca el apartado que versa sobre la promulgación de legislación específica en delito cibernético. En dicha sección, las afirmaciones son claras y contundentes: sin un marco legal y regulatorio adecuado, los Estados Miembros no pueden proteger a sus ciudadanos de los delitos cibernéticos. Es más, la resolución asevera que aquellos corren el riesgo de convertirse en refugios para los delincuentes que cometen estos delitos (Temperini, 2014).

La resolución sostiene que el Grupo de Expertos debe brindar asistencia técnica a los Estados Miembros para la aprobación de legislación que tipifiquen los delitos cibernéticos. También de leyes preventivas para que protejan los sistemas de información y eviten el uso indebido de las computadoras en actividades delictivas. Además, se insta al Grupo de Expertos a la creación de mecanismos jurídicos que impulsen la cooperación entre los investigadores, las autoridades policiales y judiciales, en casos relacionados con delitos cibernéticos.

En función de estas medidas, la resolución responsabiliza al Grupo de Expertos a gestionar el material necesario para la capacitación. Asimismo, debe brindar asistencia técnica y realizar talleres regionales, con el fin de apoyar la formulación de políticas gubernamentales

y leyes que refuercen la percepción de confianza. De esta manera, se pretende que internet sea fiable a medida que se implemente la tipificación al delito del uso indebido de computadoras y redes informáticas.

Uno de los objetivos principales de estas sesiones de capacitación trata sobre el delineamiento de leyes penales y protecciones de la privacidad. De esta manera, se prevé la realización de talleres con énfasis en la aprobación de diversas categorías de leyes: sustantivas y procesales. En cuanto a las leyes sustantivas sobre delitos cibernéticos, se manda a los Estados Miembros a la determinación de prohibiciones penales y jurídicas. En concreto, en contra de las amenazas a la confidencialidad, integridad y seguridad de los sistemas informáticos. Explícitamente, se afirma que deben considerarse ilícitas las siguientes conductas: el acceso a computadoras sin autorización, la interceptación ilícita de datos, la interferencia con la disponibilidad de sistemas informáticos, el robo y sabotaje de datos. Por consiguiente, se insta a la regulación de las mismas conforme con la normativa de cada Estado Miembro de la OEA.

En lo que respecta a las normas procesales, se hizo hincapié en la recopilación de pruebas electrónicas y se solicitó que los Estados Miembros dispusieren de procedimientos claros y alineados con las normas internacionales. El objetivo fue permitir que el gobierno acceda a comunicaciones y datos almacenados cuando sea necesario en el contexto de una investigación criminal. Igualmente, se estimó crucial garantizar a las empresas y a los consumidores que el gobierno no vigilará sus comunicaciones de manera injustificada. Así como también que los datos proporcionados por los consumidores a los comerciantes no van a ser utilizados de manera indebida.

En apoyo a la Estrategia Interamericana Integral de Seguridad Cibernética (2004), se exhortó al CICTE al desarrollo de planes para establecer una red hemisférica de CSIRT que funcione las 24 horas del día durante los 7 días a la semana. De esta manera, se debía atribuir

a la red la capacidad de divulgar rápidamente la información sobre seguridad cibernética. Así como también para la proporción de orientación y apoyo técnico en caso de incidentes cibernéticos. Cabe mencionar que el CICTE, a través de su Programa de Seguridad Cibernética (2003), se posiciona en un rol clave en este ámbito.

3.1.4. IV Reunión de Expertos Gubernamentales sobre Delito Cibernético

El siguiente hito hemisférico en la materia fue la IV Reunión de Expertos Gubernamentales sobre Delito Cibernético (2006). De acuerdo a los mandatos de la REMJA, se abordaron temas fundamentales para enfrentar los desafíos de la cooperación de las Américas en el cibercrimen. De esta forma, los expertos acordaron una serie de recomendaciones clave con el objetivo de mejorar las capacidades nacionales.

En primer lugar, se exhortó a los Estados miembros que no implementaron las recomendaciones de la reunión celebrada con anterioridad para avanzar en su ejecución de manera expedita. Además, requirió a los Estados miembros que proporcionen a la Secretaría General de la OEA la información relativa a la autoridad que representa el punto de contacto para la cooperación internacional en la materia. De acuerdo a esta información, la Secretaría General de la OEA se comprometió a la elaboración de un directorio.

Los Expertos Gubernamentales destacan los resultados de los talleres de capacitación sobre redacción de legislación específica en ciberdelito. Los talleres se realizaron en Ciudad de México, Santiago de Chile, Lima, y Nassau en el período 2004- 2005. En perspectiva de ello, se alienta a los Estados Miembros a tomar en consideración las contribuciones de los talleres para que se proyecten progresos en la adopción o adecuación de sus marcos legales. También, se destacó la importancia de desarrollar un programa de capacitación sobre la Red de Emergencia de 24 horas/7 días establecida por el G-8.

Es así que se pretendió que la asistencia a los Estados Miembros facilite la vinculación a la red 24/7. En este sentido, se subrayó que el Departamento de Justicia de Estados Unidos lidararía la organización del programa de capacitación. Se instó también a los Estados Miembros al desarrollo de la capacidad técnica y jurídica para unirse a la red 24/7 en perspectiva de colaborar en las investigaciones sobre delitos cibernéticos. Junto a esta herramienta, se recomendó que examinen otros mecanismos para fortalecer la cooperación mutua, amplia y eficiente en la materia.

Por lo que se refiere a los avances del sitio en línea de la OEA sobre la lucha contra el delito cibernético, se sugirió seguir con su desarrollo y se proclamó que debía incluirse tanto una parte pública como otra de acceso restringido para las autoridades gubernamentales. De este modo, la finalidad del portal interamericano en esta materia es que se continúe con los progresos en la consolidación de la cooperación hemisférica.

Se planteó también que la Secretaría General de la OEA siga con la recopilación y sistematización de la normativa específica sobre delito cibernético de los Estados Miembros de la OEA. En base a la información que proporcionen aquellos, se recomendó hacer hincapié en los aspectos sustantivos, procesales y de asistencia mutua. El objeto de esta medida ha sido poner a disposición esta información a disposición de los Estados Miembros de la OEA en el mencionado portal para la capacitación en la materia.

También se recomendó que la Secretaría General de la OEA confeccione un inventario de las conductas y modalidades de delito cibernético que más se cometen en la región. Para ello, resulta necesario que los Estados Miembros proporcionen información al respecto. El objeto de esta medida es la difusión de esta información en la parte privada del portal interamericano y que sea sometido para su consideración en la próxima reunión del Grupo de Expertos.

En cuanto a la capacitación a los Estados Miembros de la OEA se añadió particularmente la relativa al manejo de pruebas electrónicas y se recomendó que se progrese con el desarrollo de un programa de capacitación sobre el manejo forense de pruebas electrónicas. Se tuvo especialmente en consideración el ofrecimiento de Estados Unidos, Brasil y otros Estados de coordinar la organización de este programa. Igualmente, se sugiere el uso de programas "E-learning" para la formación constante de expertos en la materia.

Otra recomendación importante refiere a la colaboración supranacional entre la OEA, el Consejo de Europa y el Gobierno de España. En este escenario, se realizó una Conferencia Internacional sobre "La criminalidad un desafío global, una respuesta mundial", los días 12 y 13 de diciembre de 2005 que persiguió el objetivo de que los Estados Miembros de la OEA consideren la adhesión y aplicación de los principios de la Convención del Consejo de Europa sobre la delincuencia cibernética.

De igual manera, se destaca la importancia del fortalecimiento de los mecanismos de intercambio de información y cooperación con otros organismos internacionales. En concreto, se menciona a las Naciones Unidas, la Unión Europea, el APEC, la OCDE, el G-8, el Commonwealth e INTERPOL. En función de lo cual se pretende que los Estados Miembros de la OEA puedan aprovechar los desarrollos sobre la delincuencia cibernética en estos ámbitos.

Se reconoció también la necesidad de dedicar esfuerzos para la cooperación con el sector privado y las autoridades de investigación y persecución de los delitos informáticos. En esta vía, se recomendó que el Grupo de Expertos elabore una guía de mejores prácticas de asociación entre aquellos para el fomento de la prevención, investigación y sanción. En especial, se subrayó el fortalecimiento de las relaciones entre las autoridades mencionadas y las empresas proveedoras de servicios de internet (IV Reunión de Expertos Gubernamentales sobre Delito Cibernético, 2006).

3.1.5. V Reunión de Expertos Gubernamentales sobre Delito Cibernético

En la V Reunión de Expertos Gubernamentales sobre Delito Cibernético (2007) el Grupo de Expertos Gubernamentales continuó con la misma línea de recomendaciones que en las instancias anteriores. Así, se instó a los Estados Miembros a la creación de entidades especializadas en investigación y persecución de delitos cibernéticos, con equipamiento y recursos necesarios para su desempeño, se les solicitó que provean a la Secretaría General de la OEA los puntos de contacto para la cooperación internacional en delito cibernético y pruebas electrónicas y se ordenó que se siga consolidando el directorio con aquella información. De igual modo se reiteró la recomendación a los Estados Miembros que examinen sus sistemas jurídicos para el establecimiento de una legislación específica sobre delitos cibernéticos. En definitiva, se exhortó enfáticamente la adopción de medidas procesales relativas a las diversas modalidades de delitos cibernéticos y pruebas electrónicas. En el primer caso, para lograr una tipificación que garantice la investigación y persecución efectiva y la cooperación hemisférica en este ámbito. Lo mismo se insta en cuanto a asegurar la obtención, mantenimiento y admisibilidad de todas las formas de pruebas electrónicas.

> Las medidas procesales necesarias para asegurar la obtención y mantenimiento en custodia de todas las formas de pruebas electrónicas y su admisibilidad en los procesos y juicios penales y permitir la asistencia mutua entre los Estados en los asuntos relacionados con las pruebas electrónicas, incluyendo el desarrollo de reglamentaciones para los proveedores de servicios que garanticen la preservación y recuperación de la información almacenada y de tránsito (V Reunión de Expertos Gubernamentales sobre Delito Cibernético, 2007, recomendación 4).

Nuevamente, se instó a los Estados Miembros a vincularse a la red 24/7 del G-8. En este orden, se destacó los resultados satisfactorios de los talleres de capacitación sobre este

mecanismo. El mismo fue auspiciado por Estados Unidos, Brasil, Costa Rica y Barbados durante los años 2006 y 2007 para el desarrollo de la capacidad técnica y jurídica de los Estados Miembros. Esto es, con el objetivo de que puedan unirse a la red 24/7 y mejoren el manejo forense de pruebas electrónicas.

Otra recomendación solicitó a la Secretaría General que continúe con el desarrollo del Portal Interamericano de Cooperación contra el Delito Cibernético en línea. A razón de ello, los países deben suministrar información pertinente. A su vez, se aconsejó la utilización de otras herramientas tecnológicas para facilitar el flujo de información entre los expertos gubernamentales en delito cibernético y se insistió en la recopilación y publicación de la legislación específica en delito cibernético de los Estados miembros de la OEA.

En términos de cooperación internacional, se reiteró la invitación para aplicar los principios de la Convención del Consejo de Europa sobre la Delincuencia Cibernética (2005). Sobre todo, para la adopción de sistemas jurídicos que sean necesarios para su implementación con el auspicio de la Secretaría General de la OEA y el Consejo de Europa. En igual sentido, se expidió acerca de la consolidación del intercambio de información y cooperación con otros organismos internacionales referentes a delitos cibernéticos y se recomendó que en la próxima reunión se evaluaren los avances de la Estrategia Integral de Seguridad Cibernética (2004).

Se instó también a la cooperación entre las autoridades responsables de la investigación y persecución de tales delitos y el sector privado con el objetivo de fomento de estas relaciones para consolidar la prevención, investigación y sanción de los delitos cibernéticos. En este marco, se aceptó el ofrecimiento de los Estados Unidos para realizar el programa de capacitación de los Estados miembros para el desarrollo legislativo. Es decir, para la adopción de normativas y medidas procesales relacionadas con los delitos cibernéticos y las pruebas electrónicas. Finalmente, se solicitó que en la próxima reunión del Grupo se informe acerca de

los avances de este programa (V Reunión de Expertos Gubernamentales sobre Delito Cibernético, 2007).

3.1.6. VI Reunión de Expertos Gubernamentales sobre Delito Cibernético

La VI Reunión de Expertos Gubernamentales sobre Delito Cibernético (2010) evidenció marcadas continuidades en las recomendaciones de las instancias anteriores. Se mantuvieron las medidas y mismo enfoque respecto a la prevención y abordaje del delito cibernético. En este derrotero, se instó a los Estados Miembros al establecimiento de entidades especializadas y a la actualización de los puntos de contacto con el subsiguiente directorio y en lo relativo a la adopción de legislaciones específicas para la tipificación, investigación y custodia de las pruebas electrónicas. Una vez más, se exhortó a los Estados Miembros a que tomen las medidas necesarias para vincularse a la red 24/7.

Una recomendación novedosa es la que refiere a la cooperación entre los grupos de trabajo en Delito Cibernético y en Asistencia Mutua Penal y Extradición de las REMJA. En este sentido, se promocionó el flujo de información y coordinación entre aquellos y "las autoridades nacionales con responsabilidades en dichas áreas, con el fin de fortalecer la cooperación en estos campos y evitar la duplicidad de esfuerzos"(VI Reunión de Expertos Gubernamentales sobre Delito Cibernético, 2010, recomendación 8).

Otro aspecto nuevo muy destacable es la recomendación a los Estados Miembros dirigida a la protección de las computadoras y redes de los ciudadanos, las empresas y los gobiernos. En definitiva, como parte del trabajo más amplio y coordinado de la implementación de estrategias nacionales de seguridad cibernética de prevención, investigación y procesamiento de los delitos cibernéticos. Además, se profundizó la recomendación relativa al Portal Interamericano de Cooperación en materia de Delito Cibernético del sitio web de la

OEA. Más precisamente, se sugiere la incorporación de hipervínculos con las páginas de las unidades nacionales y manuales en la materia:

> Que se establezcan enlaces recíprocos entre el Portal Interamericano de Cooperación en materia de Delito Cibernético y las páginas en "Internet" que hayan establecido o establezcan en el futuro las unidades o entidades de los Estados para la investigación y procesamiento de delitos cibernéticos, y que en ellas se publiquen los manuales y cualquier otra información que se considere útil para facilitar la cooperación en las materias a su cargo (VI Reunión de Expertos Gubernamentales sobre Delito Cibernético, 2010, recomendación 7d).

En relación con lo anterior, se introdujo una recomendación que da una nueva dimensión a las estrategias nacionales y cooperación internacional. Tal como se observa en la cita anterior, se instó a los Estados Miembros al desarrollo de sitios web en línea para difundir información sobre los delitos cibernéticos. El objetivo que se plantea es la publicación de información para que sea accesible a los ciudadanos "para prevenir ser víctimas de delitos cibernéticos y para detectarlos y denunciarlos ante las autoridades competentes cuando ellos ocurran" (VI Reunión de Expertos Gubernamentales sobre Delito Cibernético, 2010, recomendación 9).

Las entidades encargadas del desarrollo de los sitios web en línea sobre los delitos cibernéticos son las entidades especializadas de cada Estado Miembro. De esta manera, la finalidad última es potenciar el desarrollo de la investigación y procesamiento de estos delitos. Asimismo, las entidades mencionadas deben trabajar en forma coordinada con la Secretaría General de la OEA para el establecimiento de los enlaces recíprocos en el Portal Interamericano de Cooperación en materia de Delito Cibernético.

Nuevamente se exhortó a la cooperación de la OEA con otros organismos supranacionales. Es así que se menciona al Consejo de Europa, las Naciones Unidas, la Unión

Europea, APEC, la OCDE, el G-8, el Commonwealth y la INTERPOL. Al igual que otras instancias, se insta a la consolidación de la cooperación entre el sector privado y las autoridades responsables del ámbito de delitos cibernéticos. También, se invita a la participación en el 12º Congreso de la ONU sobre Prevención del Delito y Justicia Penal (2010).

Al respecto de la capacitación que demanda la materia, se insistió en los talleres que se vienen realizando desde el período anterior. Ahora bien, en la VI Reunión de Expertos Gubernamentales sobre Delito Cibernético (2010) se destacó el trabajo realizado entre 2008 y 2009. En estos años, los talleres se llevaron a cabo en Puerto España, Trinidad y Tobago; Bogotá, Colombia; Santiago, Chile; Ciudad de Panamá, Panamá y Asunción, Paraguay. Al igual que sucedió con estos talleres, Estados Unidos fue el país que se ofreció como coordinador de un nuevo programa de capacitación para fiscales, investigadores y jueces.

El programa de capacitación se propuso con el objeto de mejorar y fortalecer la cooperación internacional en la investigación y procesamiento de delitos cibernéticos. Sobre todo, se hace hincapié en las tecnologías que permiten a los delincuentes utilizar internet a escala mundial y las herramientas que ayudan al cumplimiento de la ley a este respecto. En este sentido, se tiene en consideración el carácter transnacional de estos delitos y considerando las sugerencias y los intereses específicos manifestados por los Estados Miembros.

3.1.7. VII Reunión de Expertos Gubernamentales sobre Delito Cibernético

En la VII Reunión de Expertos Gubernamentales sobre Delito Cibernético (2012) se reafirmaron las recomendaciones acuñadas en las instancias anteriores y se introdujeron y consolidaron aspectos esenciales para mejorar la cooperación regional en la prevención y el combate contra el delito cibernético. En esta oportunidad, se alentaron las relaciones entre el Grupo de Trabajo en Delito Cibernético de las REMJA, la CITEL y el CICTE para avanzar en

la implementación de la Estrategia Interamericana Integral de Seguridad Cibernética (2004) según el mandato de la Asamblea General de la OEA.

Al igual que en la VI Reunión, se continuó con el proceso de profundización y actualización del Portal Interamericano de Cooperación en materia de Delito Cibernético. Una vez más, se destaca la importancia del flujo de la información a través de este sitio web, tanto en su parte pública como privada. Es por ello, que se instó a los Estados Miembros a que suministren información actualizada y respondan a las solicitudes de la Secretaría General para mantener la eficacia de este Portal. A su vez, se planteó el establecimiento de nuevos espacios virtuales para los mismos fines señalados:

> Solicitar a la Secretaría General de la OEA que, en el marco de los recursos de que dispone, continúe avanzando en el desarrollo de nuevos espacios virtuales con acceso restringido para el intercambio de información, experiencias y buenas prácticas entre los expertos gubernamentales en delito cibernético y en materia de cooperación jurídica internacional para la investigación y procesamiento de este delito (VII Reunión de Expertos Gubernamentales sobre Delito Cibernético, 2012, recomendación 8b).

Otra novedad fue la difusión de los resultados del 12º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal que la VI Reunión había instado a participar. De esta instancia surgió la Declaración de Salvador sobre estrategias amplias ante problemas globales: los sistemas de prevención del delito y justicia penal y su desarrollo en un mundo en evolución (2010). En este instrumento se invita a la Comisión de Prevención del Delito y Justicia Penal de la ONU a convocar a un grupo intergubernamental de expertos de composición abierta en delito cibernético para realizar un estudio en la materia.

Es por ello que la Declaración de Salvador es especialmente incluida entre las recomendaciones sobre cooperación internacional. Así, se pidió a los Estados Miembros que respondan un cuestionario que sería distribuido por el mencionado grupo intergubernamental

de expertos. El mismo, fue convocado como un foro de negociación multilateral por la Comisión de Prevención del Delito y Justicia Penal de las Naciones según la Asamblea General. De esta manera, se pretendió materializar lo solicitado:

> Un estudio exhaustivo del problema del delito cibernético y las respuestas de los Estados Miembros, la comunidad internacional y el sector privado ante ese fenómeno, incluido el intercambio de información sobre legislación nacional, mejores prácticas, asistencia técnica y cooperación internacional, con miras a examinar opciones para fortalecer las actuales respuestas jurídicas o de otra índole ante el delito cibernético en los planos nacional e internacional y proponer otras nuevas (Declaración de Salvador, 2010, párr. 42).

De manera análoga a la reunión anterior, la VII Reunión de Expertos Gubernamentales sobre Delito Cibernético (2012) refirió a los talleres de capacitación para fiscales, investigadores y jueces. No obstante, en esta ocasión se remitieron los resultados alcanzados en perspectiva de consolidar la cooperación internacional en la investigación y procesamiento de estos delitos. Por consiguiente, se destacaron los talleres realizados en la Ciudad de México, México; Lima, Perú; St. John's, Antigua y Barbuda; Miami, Estados Unidos; y Bogotá, Colombia, durante los años 2010 y 2011. Por último, se enfatizó en la utilidad del "Boletín de Cooperación Jurídica" elaborado y distribuido electrónicamente por el Departamento de Cooperación Jurídica de la OEA. En concreto, se relevó que su contribución fue la difusión de los progresos alcanzados por la OEA y los Estados Miembros en la cooperación contra el delito cibernético y se solicitó la continuidad de esta labor y se invita a los Estados Miembros a que contribuyan con información para el mismo.

3.1.8. VIII Reunión de Expertos Gubernamentales sobre Delito Cibernético

La VIII Reunión de Expertos Gubernamentales sobre Delito Cibernético (2014) no presentó recomendaciones novedosas en comparación con las instancias previas. Más bien, se destacó la introducción de la Secretaría Técnica de las REMJA que asume funciones que correspondían a la Secretaría General de la OEA según las reuniones anteriores. Así, la nueva entidad fue encargada de desempeñar un rol esencial de apoyo a los desarrollos legislativos de los Estados Miembros de la OEA. De este modo, se manda a la Secretaría Técnica a realizar la sistematización de las legislaciones y su publicación en el Portal Interamericano de Cooperación en materia de Delito Cibernético. Además, debe proceder a la difusión de propuestas de cooperación jurídica para el desarrollo de legislación a ser consideradas como modelo en este ámbito. También, se insta a la Secretaría Técnica a la difusión de los desarrollos en la cooperación hemisférica mediante el Boletín de Cooperación Jurídica.

En cuanto a la capacitación, se mandó que la Secretaría Técnica coordine con los Estados Unidos los talleres de capacitación, sobre todo orientados a jueces y magistrados, en consideración de las sugerencias y los intereses específicos manifestados por los Estados Miembros. En esta línea, se manifestaron los resultados de los talleres de capacitación para la cooperación internacional en la investigación y procesamiento de delitos cibernéticos. En esta oportunidad, se llevaron a cabo en Guatemala, Guatemala; Montevideo, Uruguay; Miami, Estados Unidos; y Lima, Perú; entre los años 2012 y 2013.

3.1.9. IX Reunión de Expertos Gubernamentales sobre Delito Cibernético

A partir de la IX Reunión de Expertos Gubernamentales sobre Delito Cibernético (2016) se destaca un nuevo enunciado antes de enumerar las recomendaciones acordadas. Hasta ese momento el objetivo de las recomendaciones versaba sobre la consolidación de la cooperación hemisférica en la prevención y el combate contra el delito cibernético. En esta

oportunidad, a dicha fórmula se le agrega que deben ser de conformidad con el principio de soberanía de los Estados Miembros y las legislaciones nacionales pertinentes.

Al igual que se manifestó en la VII Reunión, la mayoría de las recomendaciones se mantienen sin cambios sustanciales. Así, se actualizan los resultados alcanzados en los talleres de capacitación de jueces, magistrados, fiscales e investigadores en materia de delito cibernético. En concreto, que desde la reunión anterior se llevaron a cabo talleres en Asunción, Paraguay; Ciudad de Guatemala, Guatemala; Ciudad de Panamá, Panamá; Miami y Fort Laudardale, Estados Unidos; Brasilia, Brasil; Buenos Aires, Argentina: San José, Costa Rica; y Lima, Perú.

Un aspecto novedoso es que se insta a los Estados Miembro a la adopción de medidas para disponer de estadísticas sistematizadas anualmente en materia de investigación, persecución y sanción de los delitos cibernéticos. Asimismo, en lo que refiere a las solicitudes de asistencia mutua enviadas y recibidas en relación con delitos y los resultados obtenidos. Además, se sugiere que los Estados Miembro establezcan una entidad con la responsabilidad de asumir estas tareas y que informen a la Secretaría Técnica sus datos de contacto.

Por otro lado, se subraya la importancia de que el Grupo de Trabajo en Delito Cibernético de las REMJA se continúe fortaleciendo como un foro hemisférico. Específicamente, para que sea útil al flujo de información, de las buenas prácticas y de la cooperación entre los Estados Miembro. Sobre todo, en el ámbito de investigación, persecución y sanción de los delitos cibernéticos y manejo de evidencia digital. Otra innovación, es que se sugiere que la REMJA considere la reforma del “Documento de Washington.” El objetivo es que se permita que este grupo decida en cada reunión el momento en que estime pertinente elegir la presidencia y si elige también una vicepresidencia.

3.1.10. X Reunión de Expertos Gubernamentales sobre Delito Cibernético

La X Reunión de Expertos Gubernamentales sobre Delito Cibernético (2022) se celebró tras un intervalo de ocho años desde la realizada precedentemente. Desde 1999 nunca había transcurrido un plazo mayor de tres años entre las nueve reuniones anteriores. Además, todas se llevaron a cabo en forma presencial en la Sede de la OEA, lo que marca una diferencia significativa con la X Reunión, ya que esta fue realizada de manera virtual. También en lo relativo a las recomendaciones, debido a que la última reunión introduce más novedades en comparación con las previas.

En lo referido al Portal Interamericano de Cooperación en Delito Cibernético, se reafirman los mandatos establecidos en las reuniones anteriores. Además, se agrega una innovación respecto a la promoción del flujo de información entre universidades y centros de investigación. Así, se enfatiza en estas instituciones porque realizan investigaciones y acciones de generación de evidencia sobre delitos informáticos. Asimismo, se destacan por su contribución al desarrollo de TIC que pueden ser incluidas de modo útil y pertinente en los sistemas de administración de justicia.

Al igual que en las últimas reuniones, se subrayó la satisfacción por los resultados alcanzados en los talleres de capacitación de jueces, magistrados, fiscales e investigadores en materia de delito cibernético. Los talleres se realizaron durante el 2020-2022 en: Buenos Aires, Argentina; Santiago, Chile; Ciudad de México, México; Miami, Florida; Asunción, Paraguay; Santiago, Chile; Ciudad de Guatemala, Guatemala; Montego Bay, Jamaica; Ciudad de Panamá, Panamá; Lima, Perú; San José, Costa Rica; Quito, Ecuador; Asunción, Paraguay. Nuevamente, dichos talleres fueron liderados por Estados Unidos, el apoyo de los Estados Miembros en que se llevaron a cabo y la cooperación de la Secretaría Técnica.

De manera similar, en el ámbito de capacitaciones, se extendió el apoyo a la ejecución del programa realizado en materia de delito cibernético. Tal como en las últimas reuniones,

Estados Unidos continuó llevando a cabo los talleres en coordinación con la Secretaría Técnica. Sin embargo, el nuevo mandato introdujo consideraciones sobre el uso de las TIC y las nuevas tendencias. A su vez, instó a tener en cuenta las sugerencias y los intereses específicos manifestados por los Estados Miembros. También, se fomentó la participación de estos en el programa de capacitación, especialmente de las autoridades designadas en este ámbito (X Reunión de Expertos Gubernamentales sobre Delito Cibernético, 2022).

En cuanto a la difusión de los avances logrados por la OEA y por los Estados Miembros en la cooperación contra el delito cibernético, sigue siendo responsabilidad de la Secretaría Técnica. No obstante, en reuniones anteriores este mandato se cumplía mediante el "Boletín de Cooperación Jurídica". En esta oportunidad, se instó a que la difusión se realice a través medios electrónicos, sin especificar los canales concretos para su implantación. Al mismo tiempo, se invitó a los Estados Miembros a que contribuyan con información sobre los desarrollos en este ámbito para su posterior difusión.

Se mencionan los resultados satisfactorios por la organización de foros virtuales. Primeramente, se destacó la Cooperación Jurídica contra los Delitos Cibernéticos (2020).También, el foro de Adecuación de las Legislaciones a las Normas Internacionales contra los Delitos Cibernéticos (2020). Asimismo, aludió al foro de Criptomonedas: Desafíos a las Investigaciones y Procesamientos en Delitos Cibernéticos (2021). Y, por último, el foro de Ransomware: desafíos y cooperación internacional (2021). Esta serie de foros virtuales fueron organizadas por la Secretaría de Asuntos Jurídicos sobre El Derecho Interamericano durante la Pandemia de COVID-19.

Otro aspecto novedoso ha sido la recomendación en relación con las Reuniones de Ministros en Materia de Seguridad Pública de las Américas (MISPA). En este sentido, se instó a facilitar el conocimiento de los avances dados logrados en el marco de la MISPA, las REMJA y su Grupo de Trabajo en Cooperación Jurídica contra los Delitos Cibernéticos. Tal mandato

se fundamenta en el fortalecimiento de la cooperación hemisférica en la lucha contra estos delitos. Así como también, para que estos progresos puedan ser tenidos en cuenta, en lo que corresponda, por las autoridades de los Estados Miembros que participan en la MISPA (X Reunión de Expertos Gubernamentales sobre Delito Cibernético, 2022).

3.1.11.Portal Interamericano de Delitos Cibernéticos

Actualmente, se puede observar la materialización de las recomendaciones más importantes de las Reuniones de Expertos Gubernamentales en el Portal Interamericano de Delitos Cibernéticos (2024) de la OEA:

> El Portal Interamericano de Cooperación en Delitos Cibernéticos y el Grupo de Trabajo son dos de los mayores resultados del proceso de las Reuniones de Ministros de Justicia y otros Ministros y Fiscales Generales de las Américas (REMJA) con el objetivo de fortalecer la cooperación hemisférica en la investigación y juzgamiento de estos crímenes (párr. 1).

El sitio web de la OEA en este ámbito tiene como principal objetivo la facilitación de la cooperación y el intercambio de información entre los Expertos Gubernamentales. Al respecto de estos, sostiene que poseen responsabilidades en el área de delito cibernético o en cooperación internacional para la investigación y el enjuiciamiento. Además, agrega que los socios estratégicos de la REMJA son los Estados Unidos, a través del Departamento de Justicia y Departamento de Estado, así como también el Consejo de Europa. En este escenario, el objetivo conjunto es la promoción de medidas para el combate de los delitos cibernéticos.

Las iniciativas entre la REMJA y sus socios buscan promover mejores prácticas en el abordaje de los delitos cibernéticos. Así, incluyen capacitaciones para oficiales de gobierno para el enjuiciamiento de estos delitos y talleres legislativos para actualizar las legislaciones en la materia. Asimismo, el Portal Interamericano de Delitos Cibernéticos (2024) destaca la labor

del CICTE a través del Programa de Ciberseguridad de la OEA: asistencia técnica y capacitación, mesas redondas sobre política, ejercicios de gestión de crisis e intercambio de mejores prácticas para el uso de tecnologías de la información y la comunicación.

3.1.12.Programa de Ciberseguridad

El Programa de Ciberseguridad (2003) de la OEA es relevante en cuanto a su instrumentalidad para ayudar a los Estados Miembros en el desarrollo de estrategias nacionales de seguridad cibernética. Asimismo, en lo que refiere a la capacitación a CSIRT, tanto a nivel nacional como regional. Además, en lo relativo a la facilitación de los ejercicios de gestión de crisis en colaboración con los operadores de infraestructuras críticas, la sociedad civil y el sector privado. También, en la concientización sobre las amenazas y las oportunidades relacionadas con la seguridad cibernética en nuestra región.

A pesar de estos esfuerzos, sigue existiendo una escasez de literatura integral sobre seguridad cibernética en América Latina y el Caribe. Para abordar esta necesidad, el Programa de Seguridad Cibernética del CICTE de la OEA se dedica desde el año 2013 a difundir información en colaboración con líderes en esta materia. Así, se publica una serie de informes que proporciona una visión detallada y actualizada del panorama de la seguridad cibernética y la delincuencia cibernética en la región (Observatorio de la ciberseguridad en América Latina y el Caribe, 2016).

De acuerdo al Portal Interamericano de Delitos Cibernéticos (2024), el Programa de Ciberseguridad se posiciona como el líder regional que brinda asistencia a los Estados miembros de la OEA en el desarrollo de capacidades de ciberseguridad. Desde el ámbito de políticas públicas como a nivel técnico, sus iniciativas y actividades promocionan la existencia de un ciberespacio abierto, seguro y resistente en todo el hemisferio occidental. En este orden, sus objetivos son:

- Apoyar a los Estados Miembros de la OEA en el desarrollo de capacidades técnicas y políticas para prevenir, identificar, responder y recuperarse exitosamente de incidentes cibernéticos.
- Mejorar el intercambio de información, la cooperación y la coordinación sólidas, efectivas y oportunas entre las partes interesadas en seguridad cibernética a nivel nacional, regional e internacional.
- Aumentar el acceso al conocimiento e información sobre amenazas y riesgos cibernéticos por parte de los interesados públicos, privados y de la sociedad civil, así como los usuarios de Internet.

Por lo que se refiere a las actividades del Programa de Ciberseguridad, se destaca:

- El desarrollo de políticas: porque ayuda a los Estados miembros en el desarrollo de estrategias nacionales de ciberseguridad. En estas medidas se involucran a todas las partes interesadas y relevantes en el ámbito. Además, las estrategias nacionales se adaptan a la situación legislativa, cultural, económica y estructural de cada Estado Miembro.
- La creación de capacidades: porque colabora en el establecimiento de CSIRT y brinda asistencia técnica personalizada y oportunidades de capacitación para fortalecer las instituciones y organizaciones nacionales. Adicionalmente, cuenta con la red CSIRTAmericas, la cual brinda inteligencia sobre amenazas y tendencias cibernéticas en la región.
- La investigación y divulgación: porque desarrolla documentos técnicos, herramientas e informes para orientar a los responsables de la formulación de políticas, los CSIRT, los operadores de infraestructura, las organizaciones privadas y la sociedad civil. Asimismo, difunde los avances actuales e identifica problemas y desafíos clave de ciberseguridad en la región.

De este modo, las Américas se encuentran en un continuo avance hacia la construcción de una confianza digital. Sin embargo, la frecuencia de los ataques cibernéticos no deja de

aumentar en relación al crecimiento exponencial de las tecnologías. Por lo tanto, la cuestión de la seguridad cibernética sigue su proceso de ampliación hacia dimensiones transversales en el análisis de estos delitos. La OEA registra los progresos de los Estados Miembros que actualizaron sus marcos jurídicos, a partir de lo cual se fue incluyendo la tipificación del ciberhostigamiento, el ciberacoso, el grooming y el ciberbullyng y la distribución no consentida de imágenes íntimas o sexuales (OEA, 2021).

3.1.13.Grupo de Trabajo

La REMJA estableció el Grupo de Trabajo en 1999 como el principal foro hemisférico para consolidar la cooperación internacional. En esta línea, los ámbitos se refieren a la prevención, investigación y enjuiciamiento de los delitos cibernéticos, al intercambio de información y experiencias entre sus miembros. En perspectiva de ello, el objetivo es delinear recomendaciones para el fortalecimiento de la cooperación entre los Estados miembros de la OEA y otros organismos internacionales.

De esta forma, el Grupo de Trabajo promueve la adopción o actualización de legislaciones nacionales y medidas procesales para la persecución efectiva de los delitos cibernéticos, así como las reglamentaciones para que los proveedores de servicios de internet aseguren la preservación y recuperación de la información almacenada y de tránsito. A su vez, promueve en los Estados Miembros el desarrollo de estrategias nacionales que incluyan esfuerzos para prevenir, investigar y procesar los delitos cibernéticos.

En suma, los objetivos del Grupo de Trabajo son:

- Facilitar el intercambio de información y de experiencias.
- Fortalecer la cooperación entre las autoridades especializadas en estos delitos.

- Capacitar a jueces y fiscales de las Américas en el manejo de evidencia electrónica y en la investigación y juzgamiento de estos delitos (Portal Interamericano de Delitos Cibernéticos, 2024).

3.1.14.El Programa de Capacitación

La capacitación de las Américas es otra de las recomendaciones más destacadas en las sucesivas reuniones del Grupo de Expertos. Ante los desafíos excepcionales que presentan los delitos cibernéticos se formuló el Programa de Capacitación para el beneficio de los Estados Miembros. Tal como se advirtió en apartados anteriores, Estados Unidos a través del Departamento de Justicia auspicia esta labor, promueve las buenas prácticas, la distribución del conocimiento y de las técnicas para investigar, juzgar y adjudicar delitos cibernéticos.

De acuerdo al Portal Interamericano de Delitos Cibernéticos (2024) se realizaron más de 40 talleres, con más de 2.500 jueces y fiscalías de las Américas. Además, su formato y contenido se replicaron en las capacitaciones nacionales de jueces y fiscales. En este marco, se subraya que los talleres poseen un enfoque holístico basado en tres aspectos:

- Investigación: incluye técnicas de análisis de evidencia, capacitación sobre combinación de métodos de investigación tradicional con nuevas tecnologías.
- Persecución: refiere a la capacitación sobre presentación de la evidencia en una corte judicial.
- Evaluación y análisis: relativo a la capacitación sobre el análisis de la evidencia que se presenta y para garantizar que no fue alterada. También aborda la actualización de la legislación existente en relación con los crímenes modernos.

Por otro lado, en el Portal Interamericano de Delitos Cibernéticos (2024) se destacan las tres características principales de los talleres:

- Casos de estudio: a través de trabajo en equipos se posibilita la aplicación de lo aprendido durante el taller en un caso de la vida real.
- Networking: en los talleres se crean redes en la región para conectar a los participantes entre sí. De esta manera, se obtienen conocimientos al mismo tiempo que se establecen contactos judiciales y fiscales para interactuar e intercambiar información y buenas prácticas.
- Cursos para distintos niveles de público: los talleres están en constante desarrollo para captar las necesidades de la región. Los temas son elegidos en base a los participantes y su nivel de conocimiento. En este sentido, se imparten distintos talleres de nivel básico, para aquellos que tuvieron poco contacto con el tema, y cursos más avanzados para aquellos que participaron previamente del programa.

3.1.15.Departamento de Cooperación Jurídica

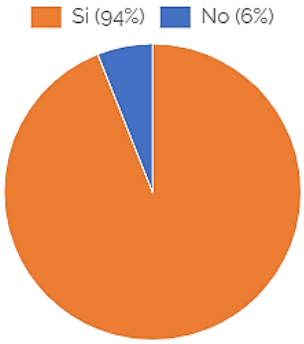
El Departamento de Cooperación Jurídica como Secretaría Técnica del Grupo de Trabajo en Materia de Delito Cibernético de la REMJA tiene como función la recopilación estadística. En esta labor, reúne datos e información legislativa específica sobre delito cibernético para la realización de un diagnóstico de los Estados miembros. En este marco, son asistidos por la Oficina del Fiscal General, el Ministerio Público y Oficinas Judiciales. También, es de vital colaboración, las Misiones Permanentes de la OEA, que compilan y comparte la información con el Departamento de Cooperación Jurídica. En el Portal Interamericano de Delitos Cibernéticos se presentan los resultados sobre legislación, tendencias emergentes y las herramientas de cooperación internacional hasta el año 2020.

3.1.16.Legislación sustantiva

El 94% de los Estados Miembros tiene normativas que abordan los ataques a la integridad de datos. De esta manera, esta legislación sustantiva se destaca porque 33 de los 35

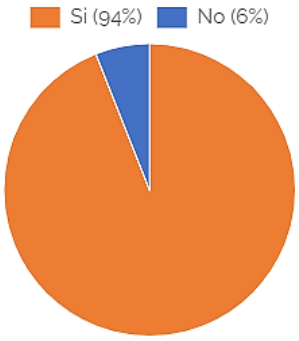
Estados Miembros de la OEA lo incluyeron en sus sistemas jurídicos. En contraste, el restante 6% no cuenta con legislación específica para estos delitos que se cometen con la intención de modificar, alterar o eliminar datos informáticos de manera no autorizada. También, el fraude informático y la pornografía infantil son los más legislados por los Estados Miembros. Estos delitos presentan el mismo porcentaje de inclusión como legislación sustantiva que el referente a los ataques a la integridad de datos.

Gráfico 3. Ataques a la integridad de datos



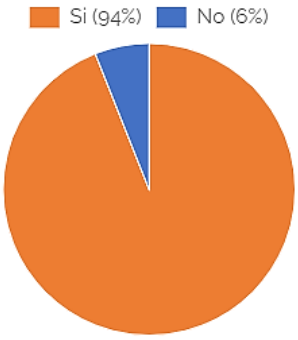
Nota. Portal Interamericano de Delitos Cibernéticos (2020)

Gráfico 4. Fraude informático



Nota. Portal Interamericano de Delitos Cibernéticos (2020)

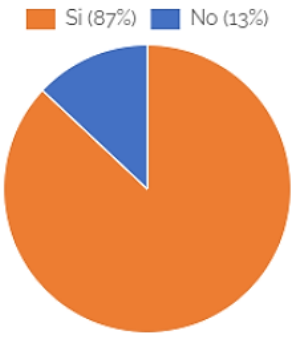
Gráfico 5. Pornografía infantil



Nota. Portal Interamericano de Delitos Cibernéticos (2020)

Por otro lado, la gran mayoría de los Estados Miembros posee legislación sustantiva sobre acceso ilícito. Así, el 87% que representa a 30 Estados Miembros tiene en su sistema jurídico el acceso no autorizado a sistemas o datos informáticos. Por lo tanto, el 13% que refiere a 5 Estados Miembros no dispone específicamente de esta normativa.

Gráfico 6. Acceso Ilícito

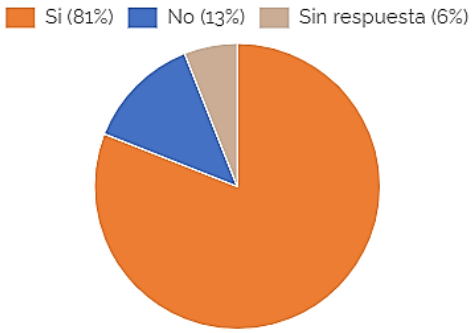


Nota. Portal Interamericano de Delitos Cibernéticos (2020)

En su mayoría, los Estados Miembros poseen legislación sustantiva sobre interpretación ilícita de información o datos con la intención de cometer delitos informáticos. En este sentido, el 81%, que equivale a 28 Estados Miembros, cuenta con un sistema jurídico que regula la interpretación ilícita de datos informáticos. Asimismo, el 13%, es decir 5 Estados Miembros,

no legisla en la materia. Al respecto del 6 % restante, que representa a 2 Estados Miembros, no existe información disponible en esta área específica.

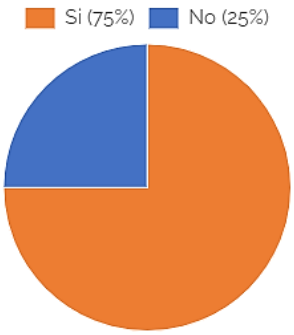
Gráfico 7. Interpretación ilícita



Nota. Portal Interamericano de Delitos Cibernéticos (2020)

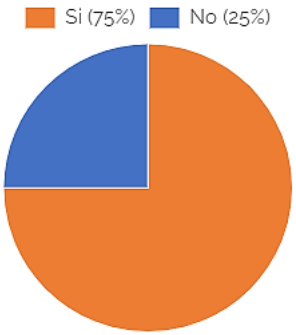
En cambio, la legislación sustantiva que versa sobre ataques a la integridad de sistemas se reduce al 75% de los Estados Miembros. Es decir que, en el marco de la OEA, solamente 26 países disponen de normativas que regulen este tipo de delitos. Por lo tanto, el 25%, que es igual a 9 Estados Miembros, no disponen de una normativa específica para este tipo de ilícitos. Las mismas cifras se evidencian en el caso del delito de falsificación informática.

Gráfico 8. Ataques a la integridad de sistemas



Nota. Portal Interamericano de Delitos Cibernéticos (2020)

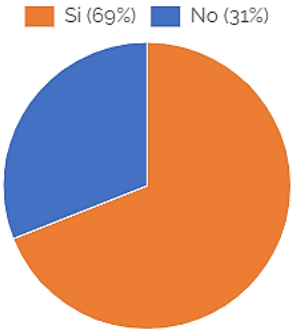
Gráfico 9. Falsificación informática



Nota. Portal Interamericano de Delitos Cibernéticos (2020)

En cuanto al delito de abuso de dispositivos, las estadísticas descienden hasta el 69%, es decir que, 24 Estados Miembros tienen legislación sustantiva en el área. En contraste, el 31% de los Estados Miembros de la OEA no evidencian su regulación.

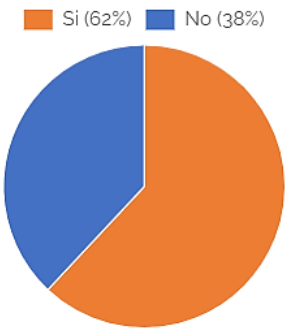
Gráfico 10. Abuso de dispositivos



Nota. Portal Interamericano de Delitos Cibernéticos (2020)

Por lo que se refiere a los delitos contra la propiedad intelectual y derechos afines, solamente el 62% lo incluye en su legislación sustantiva. En otras palabras, 22 Estados Miembros tienen normativas específicas sobre estos ilícitos en contraste con el 38%, es decir 13 países de la OEA.

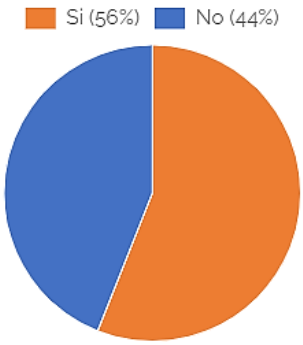
Gráfico 11. Delitos contra la propiedad intelectual y derechos afines



Nota. Portal Interamericano de Delitos Cibernéticos (2020)

A continuación, se destaca que alrededor de la mitad de los 35 Estados Miembros regula el delito de tentativa de comisión de un delito cibernético. En concreto, se trata del 56% que representa a 20 Estados Miembros. En consecuencia, el 44% no lo incluye en su legislación específica, que equivale a 15 países pertenecientes de la OEA.

Gráfico 12. La tentativa de comisión de un delito cibernético

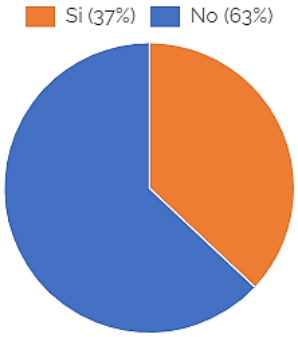


Nota. Portal Interamericano de Delitos Cibernéticos (2020)

En menor medida se encuentra regulado el delito de complicidad en la comisión de un delito cibernético. En este sentido, el 37% lo incluyen en su legislación sustantiva, es decir solamente 13 Estados Miembros. Por lo tanto, el 63% restante, que representa a la mayoría de

los Estados Miembros, no dispone de una normativa específica para este tipo de delitos en sus sistemas jurídicos.

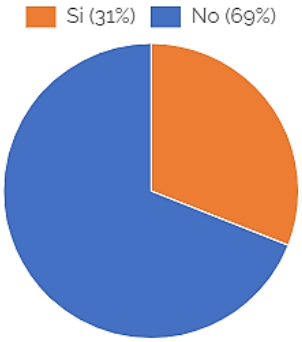
Gráfico 13. La complicidad en la comisión de un delito cibernético



Nota. Portal Interamericano de Delitos Cibernéticos (2020)

Por último, el delito de responsabilidad corporativa es el tipo de ilícito menos incluido en la legislación sustantiva de los Estados Miembros. De esta manera, tan sólo el 31%, que equivale a 11 Estados Miembros, dispone de regulación específica al respecto. Por consiguiente, el 69%, que es la mayoría de aquellos, no incluyen el delito de responsabilidad corporativa en sus sistemas jurídicos.

Gráfico 14. Responsabilidad corporativa

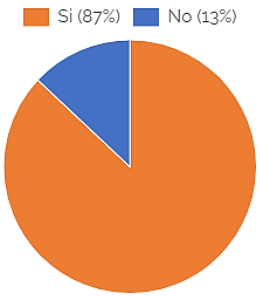


Nota. Portal Interamericano de Delitos Cibernéticos (2020)

3.1.17. Legislación procesal

En el ámbito de legislación procesal, el 87% regula la confiscación de sistemas o dispositivos de almacenamiento informáticos. En este sentido, 30 Estados Miembros, que equivale a una amplia mayoría, cuenta con esta normativa. En contraste, el 13% restante, es decir, 5 Estados Miembros no disponen de la misma.

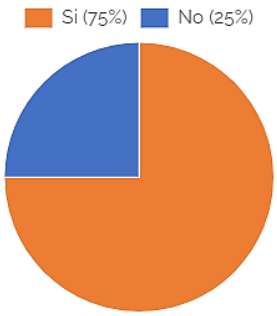
Gráfico 15. Confiscar sistemas o dispositivos de almacenamiento informáticos



Nota. Portal Interamericano de Delitos Cibernéticos (2020)

El siguiente ámbito que se encuentra más regulado es el registro, copia y acceso a los datos almacenados en un sistema informático. Así el 75%, que representa a 26 Estados Miembros, dispone de esta legislación procesal en su marco jurídico. Por lo tanto, el 25 %, que equivale a 9 Estados Miembros, no cuenta con esta normativa.

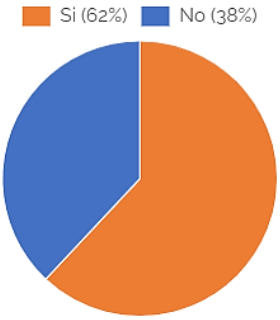
Gráfico 16. Registrar, copiar, y acceder a los datos almacenados en un sistema informático



Nota. Portal Interamericano de Delitos Cibernéticos (2020)

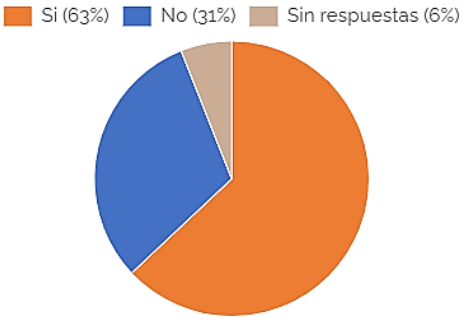
Por su parte, el 62% de los Estados Miembros mandan que los proveedores de servicios de internet produzcan datos pertenecientes a uno de sus usuarios a las fuerzas del orden público para su registro y/o incautación. Es decir, 2 países de la OEA disponen de esta legislación procesal mientras que el 38% no lo regula, lo que equivale a 13 Estados Miembros. De manera análoga se encuentra la autorización para realizar un registro remoto a través de un sistema informático. En este caso, el 63% de los Estados Miembros tienen legislación sustantiva que lo regula.

Gráfico 17. Requerir que los proveedores de servicios de internet produzcan datos pertenecientes a uno de sus usuarios a las fuerzas del orden público para su registro y/o incautación



Nota. Portal Interamericano de Delitos Cibernéticos (2020)

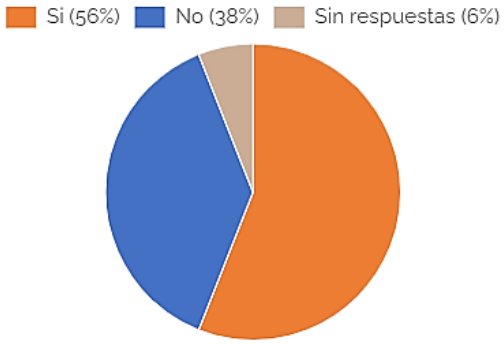
Gráfico 18. Recibir autorización para realizar un registro remoto a de un sistema informático



Nota. Portal Interamericano de Delitos Cibernéticos (2020)

Luego, el 56% dispone la legislación procesal para la compilación y certificación de la recopilación de evidencia digital a partir de información disponible públicamente en un sitio web o sitio de redes sociales. En otras palabras, alrededor de la mitad de los Estados Miembros disponen de esta regulación específica en la materia. Mientras que el 38%, que representa a 15 Estados Miembros, no cuentan con esta normativa. En cuanto al 6% restante, no se dispone de información al respecto.

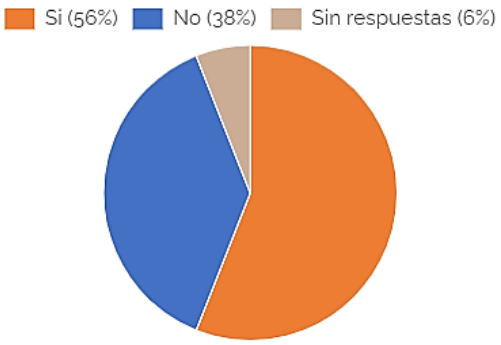
Gráfico 19. Recopilación de evidencia digital a partir de información disponible públicamente



Nota. Portal Interamericano de Delitos Cibernéticos (2020)

En cuanto a los procedimientos establecidos para garantizar la cadena de custodia de las evidencias electrónicas para garantizar su integridad, el 56% cuenta con esta legislación procesal. Es decir, 20 Estados Miembros regulan este procedimiento en contraste con el 38%, que equivale a 13 Estados Miembros. Asimismo, no se dispone de información acerca del 6% restante.

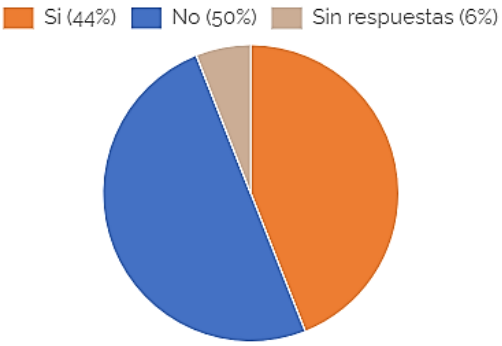
Gráfico 20. Procedimientos establecidos para garantizar la cadena de custodia de las evidencias electrónicas o para garantizar su integridad



Nota. Portal Interamericano de Delitos Cibernéticos (2020)

En relación a la recolección de información de herramientas de fuentes abiertas, solamente el 44% cuenta con legislación procesal, es decir 15 Estados Miembros. Además, exactamente la mitad de aquellos, que equivale a 18 Estados Miembros, no disponen de regulación en la materia. Por lo cual, el 6% restante, que representa a 2 Estados Miembros, no revela información al respecto.

Gráfico 21. Recolectar información de herramientas de fuentes abiertas

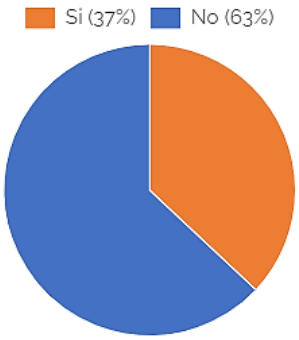


Nota. Portal Interamericano de Delitos Cibernéticos (2020)

El monitoreo en tiempo real de los datos de tráfico y la conservación de evidencias de tipo electrónico sin necesidad de una orden de allanamiento de un tribunal son regulados por

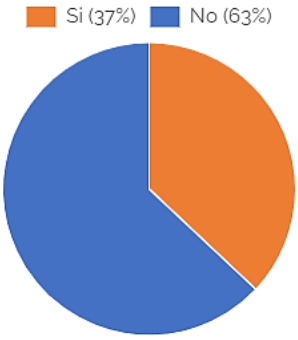
el 37%. Por lo tanto, 13 Estados Miembros disponen de legislación procesal para ambos aspectos. En cambio, el 63%, que equivale a 22 Estados Miembros, no cuentan con estos procedimientos.

Gráfico 22. Realizar monitoreo en tiempo real de los datos de tráfico



Nota. Portal Interamericano de Delitos Cibernéticos (2020)

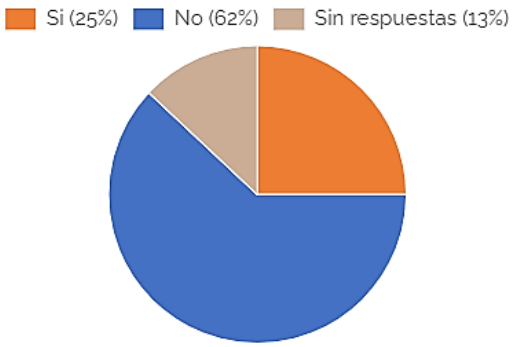
Gráfico 23. Conservación de evidencias electrónicas sin una orden de allanamiento



Nota. Portal Interamericano de Delitos Cibernéticos (2020)

La regulación para realizar una interceptación de contenido en tiempo real es la que menos se encuentra en la legislación procesal de los Estados Miembros. De este modo, solamente el 52% regula este aspecto en específico, es decir 9 Estados Miembros. Es así que el 62% no cuenta con este procedimiento, que equivale a 22 Estados Miembros. Por último, se desconoce información acerca del 13% de los Estados Miembros restantes.

Gráfico 24. Realizar una interceptación de contenido en tiempo real

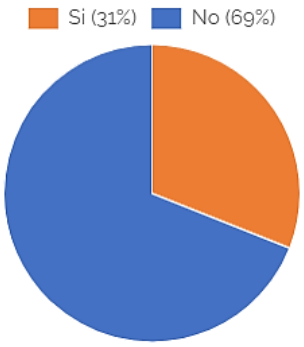


Nota. Portal Interamericano de Delitos Cibernéticos (2020)

3.1.18.Tendencias emergentes

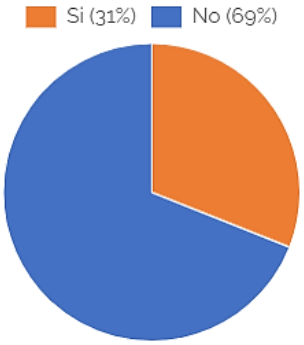
El acoso cibernético y la difusión de contenido íntimo sin consentimiento presentan el mayor porcentaje por lo que se refiere a las tendencias emergentes. De todas formas, solamente el 31%, que equivale a 11 Estados Miembros, otorgan relevancia a la legislación sobre este ciberataque. Por lo tanto, el 69%, que representa a 24 Estados Miembros, no cuenta con regulación específica en la materia.

Gráfico 25. Acoso cibernético



Nota. Portal Interamericano de Delitos Cibernéticos (2020)

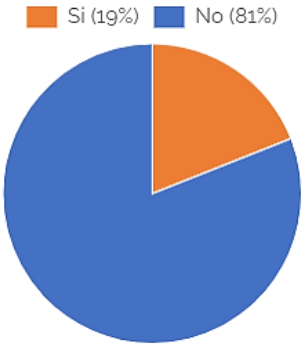
Gráfico 26. Difusión de contenido íntimo sin consentimiento



Nota. Portal Interamericano de Delitos Cibernéticos (2020)

A continuación, se destaca que el 19% de los Estados Miembros dispone de legislación sobre asedio cibernético. Es decir, únicamente 7 de los países de la OEA forman parte de esta tendencia emergente en delitos cibernéticos. En contraste, 28 Estados Miembros no regulan específicamente el asedio cibernético, lo que constituye una amplia mayoría.

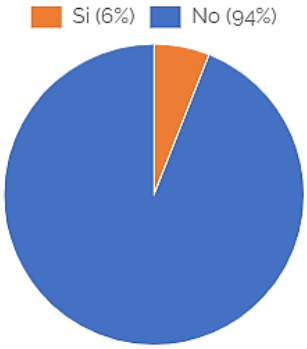
Gráfico 27. Asedio cibernético



Nota. Interamericano de Delitos Cibernéticos (2020)

La tendencia emergente que presenta menos legislación es el delito cibernético de ingeniería social. Así, tan sólo el 6%, que representa a 2 Estados Miembros, regulan este tipo de ilícito. En cambio, casi la totalidad de aquellos, que equivale a 33 Estados Miembros, no cuentan con normativas específicas para el abordaje de este delito.

Gráfico 28. Ingeniería social

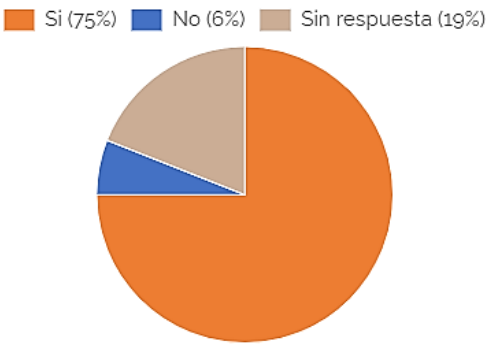


Nota. Portal Interamericano de Delitos Cibernéticos (2020)

3.1.19. Cooperación Internacional

En el ámbito de cooperación internacional la medida que manifiesta mayor prevalencia es el proceso de solicitudes de asistencia mutua de otro/s Estado/s Miembro/s con el fin de obtener evidencia digital ubicada en su país. De este modo, el 75%, que equivale a 26 Estados Miembros, evidencia voluntad de cooperación en este sentido. Luego, el 6%, que representa a 2 Estados Miembros, no cuentan con esta regulación en sus sistemas jurídicos. El 19% restante, es decir 7 Estados Miembros, no dispone de información al respecto.

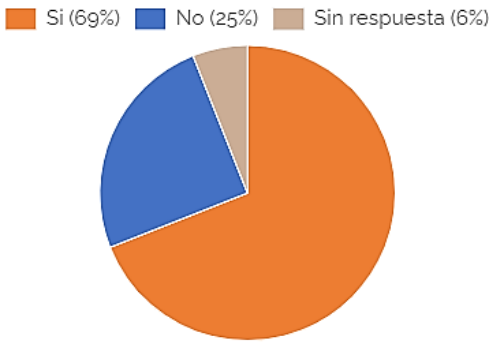
Gráfico 29. Procesar las solicitudes de asistencia mutua de otros Estados con el fin de obtener evidencia digital ubicada en su país



Nota. Portal Interamericano de Delitos Cibernéticos (2020)

En orden de preeminencia porcentual, se encuentra la realización de solicitudes de asistencia mutua a otros países para la investigación o persecución de delitos cibernéticos. El fin de esta medida es la obtención de pruebas en formato electrónico y la realización de otros actos necesarios para facilitar la investigación o persecución de estos delitos. Es así que, el 69%, que equivale a 24 Estados Miembros, encauza esta forma de cooperación. En cambio, el 25%, que representa a 9 Estados Miembros, no lo incluye en sus sistemas jurídicos. El 6% restante, es decir 2 Estados Miembros, no dispone de información al respecto.

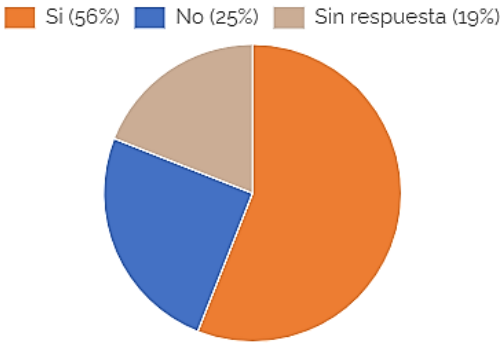
Gráfico 30. Realización de solicitudes de asistencia mutua a otros Estados Miembros



Nota. Portal Interamericano de Delitos Cibernéticos (2020)

Se relevó que el 56% dispone de medidas para el recibimiento de solicitudes de asistencia mutua para la investigación o persecución de delitos cibernéticos y para la obtención de pruebas en formato electrónico y la realización de otros actos necesarios para facilitar la investigación o persecución de estos delitos. Es decir, 20 Estados Miembros evidencian voluntad de cooperación internacional en este aspecto en específico. En contraste, el 25%, que representa a 9 Estados Miembros, no adhiere a esta medida. El 19% restante, que equivale a 6 Estados Miembros, no dispone de información al respecto.

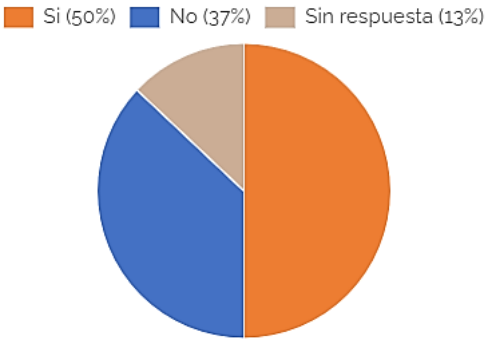
Gráfico 31. Recibimiento de solicitudes de asistencia mutua de otros Estados Miembros



Nota. Portal Interamericano de Delitos Cibernéticos (2020)

En cuanto a la Red G7 24/7 para delitos de alta tecnología, cabe decir que la mitad de los Estados Miembros se encuentran adheridos. En concreto, 18 Estados Miembros forman parte de la Red 24/7 que se acordó en el marco del G7 en contraste con el 37%, que equivale a 13 Estados Miembros. Mientras que, el 13% restante no dispone de información al respecto, es decir, sobre 4 Estados Miembros.

Gráfico 32. La Red G7 24/7 para Delitos de Alta Tecnología



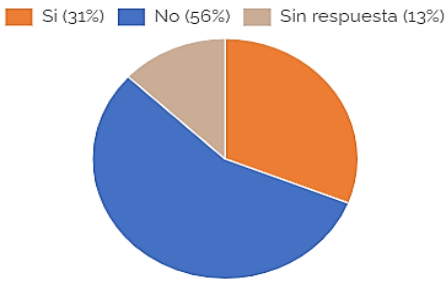
Nota. Portal Interamericano de Delitos Cibernéticos (2020)

Todavía cabe señalar que existe menor adhesión a la Red 24/7 de la Convención de Budapest sobre la Ciberdelincuencia. De esta manera, solamente el 31%, que representa a 11 Estados Miembros, forman parte de aquella. En cambio, el 56%, que equivale a 20 Estados

Miembros no se encuentran adheridos. Así, el 13% restante no presenta información al respecto, es decir 4 Estados Miembros.

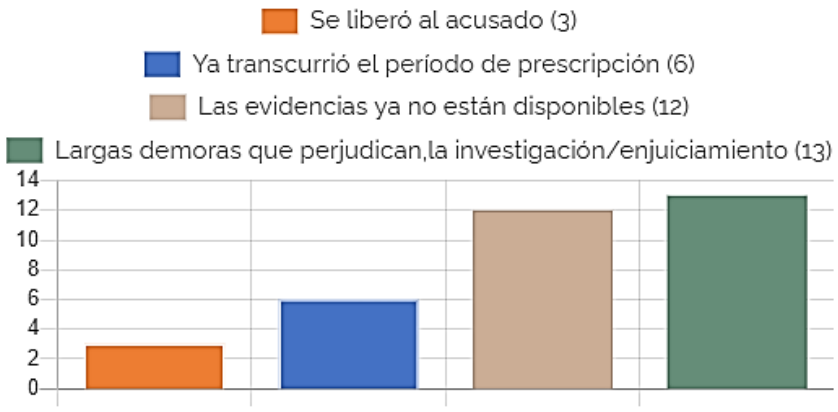
Además, en el ámbito de coordinación internacional se relevan las dificultades más usuales cuando un fiscal solicita pruebas electrónicas a través de asistencia jurídica mutua. En este sentido, las problemáticas que más se reportan son las largas demoras que perjudican la investigación o enjuiciamiento, así como también que las evidencias ya no estén disponibles. Luego, en menor medida, otras dificultades más comunes suelen que transcurrió el período de prescripción o que se liberó al acusado.

Gráfico 33. La Red 24/7 organizada bajo la Convención sobre la Ciberdelincuencia



Nota. Portal Interamericano de Delitos Cibernéticos (2020)

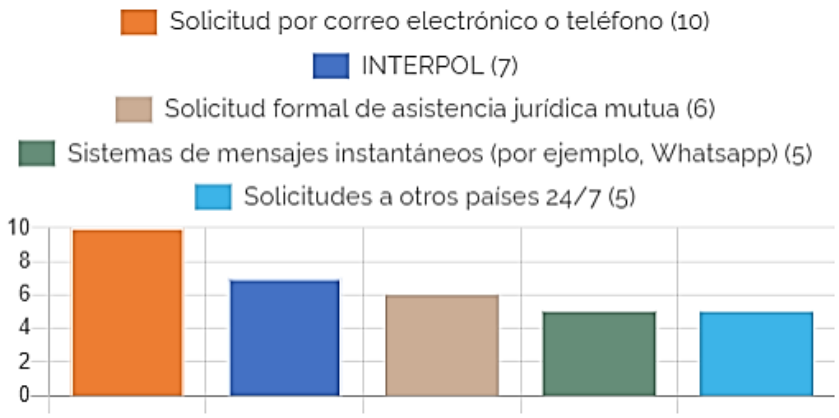
Gráfico 34. Dificultades más comunes cuando un fiscal solicita pruebas electrónicas a través de asistencia jurídica mutua



Nota. Portal Interamericano de Delitos Cibernéticos (2020)

Finalmente, en el ámbito de cooperación internacional se destacan los medios menos formales para la preservación de pruebas en formato electrónico en un Estado Miembro. En primer lugar, se releva la solicitud por correo electrónico o teléfono. A continuación, se subraya a la INTERPOL y a la solicitud formal de asistencia jurídica mutua. Así como también, los sistemas de mensajes instantáneos y las solicitudes a otros Estados Miembros a través de la Red 24/7.

Gráfico 35. Medios menos formales para la preservación de pruebas electrónicas en un Estado Miembro



Nota. Portal Interamericano de Delitos Cibernéticos (2020)

CAPÍTULO IV

LOS DELITOS INFORMÁTICOS EN EL ORDENAMIENTO JURÍDICO ARGENTINO. ANÁLISIS LEGISLATIVO

A través de la legislación se busca la sanción e implementación de normas que puedan prever y resolver ciertas necesidades y requerimientos de una sociedad en un espacio y tiempo determinados. Inclusive, el legislador puede vislumbrar la posibilidad de proyectar una ley hacia el futuro, con una visión adelantada a los tiempos legislativos. No obstante, la regla general es que es casi imposible prever la magnitud de los cambios que se avecinan. Más bien, a medida que la sociedad evoluciona la legislación debe adaptarse para proporcionar las respuestas que se necesitan en el contexto en que se encuentra.

En este marco es claro que la idoneidad de los delitos tipificados por el legislador del siglo pasado no es acorde con el tratamiento que la delincuencia informática demanda en la actualidad. El Código Penal originario no abarcaba la regulación de figuras delictivas de la magnitud que hoy en día se necesitan para dar respuesta eficaz a los avances tecnológicos y su utilización ilícita. La realidad es evidente: en el siglo XXI existen conductas ilícitas que no pueden subsumirse en las figuras penales desfasadas, lo cual impone la necesidad de gestar nuevas tipificaciones legales. Caso contrario, la sanción sería inapropiada porque no corresponde con la gravedad del hecho encuadrado en el tipo penal (Arocena, 2012). En efecto, el derecho tiene la función de regular las relaciones sociales entre los particulares y entre aquellos y el propio Estado en el momento en que esas normas se formulan. En la actualidad los delitos informáticos requieren la determinación precisa de los nuevos tipos delictivos, la forma que éstos adquieren y los medios de su comisión en la era digital. En el caso de Argentina, la gradual expansión tecnológica no fue acompañada de una evolución legislativa acorde. Si bien existieron muchos intentos de actualización legislativa en la materia, ninguno

fue sancionado (Figari, 2009). En efecto, gran cantidad de proyectos de ley sobre delitos informáticos perdieron vigencia en Argentina. Sin embargo, la Ley N° 26388 surge del tratamiento de varios expedientes legislativos y aparece como una versión mejorada y refinada de todas las iniciativas desde 1996 hasta 2008 (Rosende, 2008 y Filia et al., 2008):

- En 1994, los proyectos de ley que plantean la incorporación del delito de intrusión en el Código Penal Argentino.
- El proyecto de ley sobre delitos informáticos sobre la incorporación en el Art. 77 de terminología y definiciones en la materia. También, a la violación de secreto (Arts. 153, 154 y 157), estafas y otras defraudaciones (Arts. 173 y 175 inc. 2º), daño (Arts. 183 y 185), interrupción de las comunicaciones (Arts. 194, 195, 197), delitos que comprometen la paz y dignidad de la Nación (Arts. 222 y 225) y delitos de propiedad intelectual (Art. 72 ter. de la ley 11.723).
- El proyecto de ley sobre la incorporación de una ley complementaria con 3 artículos vinculados con la comisión de los tipos de hurto y daño a través de medios informáticos.
- El proyecto de ley versaba sobre 5 artículos para la regulación de las figuras de hurto, estafa y daño a través de medio informático y agravaba las conductas cuando fueran perpetradas por funcionarios públicos.
- En 1997, el proyecto de ley sobre el Régimen Penal del Uso Indebido de Computación que contenía nueve capítulos. En el mismo año, el proyecto de Ley Penal y Protección de la Informática que incluía 43 artículos.
- En 1998, el proyecto de ley sobre delitos informáticos.
- En 2000, el proyecto de ley sobre apropiación de mensajes y registros enviados por correo electrónico.
- En 2001, el proyecto de ley sobre delitos informáticos que buscaba la incorporación de tres tipos básicos: acceso ilegítimo informático, daño informático y fraude informático.

- En 2005, el anteproyecto de delitos informáticos que tenía dieciséis artículos entre los cuales se sugería la regulación de los delitos autónomos, entre ellos: daño informático, estafa informática, delitos contra la privacidad y ofrecimiento o difusión de pornografía infantil.
- En 2006 se presentaron 6 proyectos de ley, de los cuales dos iniciativas proponen equiparar el correo electrónico a la correspondencia epistolar. Una tercera propuesta versaba sobre modificaciones al tipo penal de violación de secreto e introducía un nuevo bien jurídico: la privacidad. Puntualmente, contemplaba los siguientes dispositivos legales: artículos 153, 154, 154 bis, 155, 156, 157, 157 bis e incorporación de los artículos 154 ter y 157 ter. Otro proyecto de ley punía expresamente el ofrecimiento y difusión de la pornografía infantil y prostitución infantil. Luego, un quinto proyecto de ley introducía modificaciones a los tipos penales de estafa y daño (artículos 173, inciso 15, 183 y 184). Y, la última propuesta instituía una ley especial o complementaria que contenía cinco capítulos: Capítulo I.- Acceso ilegítimo informático; Capítulo II.- Violación al correo electrónico; Capítulo III.- Daño informático; Capítulo IV.- Fraude informático y Capítulo V.- Pornografía infantil.

Aunque, como se mencionó con anterioridad, todos estos proyectos de ley no fueron en vano porque sentaron precedentes para las nuevas bases normativas. Especialmente, los intentos de regulación específica sobre delitos informáticos nutrieron la sanción de la Ley N° 26388 (2008). No obstante, su importancia, sirvieron como impulso inicial en la continua evolución legislativa que demanda la problemática. De hecho, la adecuación de la normativa argentina a los parámetros internacionales en la materia demanda constantemente un arduo trabajo al legislador (Celli Triunfetti, 2019).

Antes de avanzar en el análisis de la legislación más reciente, se debe hacer hincapié en disposiciones anteriores, particularmente en aquellas que de alguna manera se encuentran vinculadas con los delitos cometidos mediante el uso de las tecnologías. En este orden se

destacan muy especialmente la Ley N° 11723 de Propiedad Intelectual y la Ley N° 25326 de Protección de Datos Personales.

4.1. Ley N° 11723 de Propiedad Intelectual

La Ley N° 11723 (1933) protege los derechos de los autores de obras científicas, literarias, artísticas o didácticas (Portal Oficial del Estado Argentino, s.f.). Además de regular el derecho de Propiedad Intelectual, contiene disposiciones sobre el fomento del libro y la lectura. También, incluye disposiciones sobre el dominio público pagante, la gestión de derechos colectivos de autores y de titulares de derechos conexos.

La Ley de Propiedad Intelectual se modificó en distintas oportunidades de acuerdo a la necesidad de actualización de la norma a la realidad social. En este marco, se sancionaron las leyes 12063 (1957), 24249 (1993) y 25036 (1998), que modificaron los artículos 1, 4, 5, 8, 9, 30, 34, 57 59 y 84. Asimismo, se elevaron los montos de las penas de los artículos 73, 74 y 74 BIS según la Ley N° 11723 (1933) según la Ley N° 17.567 (1968), la Ley N° 20.509 (1973), la Ley N° 22.461 (1981), la Ley 22.936 (1983), la Ley N° 23.077 (1984), la Ley N° 23.479 (1987) y La Ley N° 23.974 (1991).

En el artículo 1 se define con precisión que las obras protegidas comprenden a los escritos de toda naturaleza y extensión. De este modo, incluye los programas de computación y las compilaciones de datos o de otros materiales. También, abarca a las obras dramáticas, composiciones musicales, dramático-musicales, las cinematográficas, coreográficas y pantomímicas. También están incluidas dentro de la tutela normativa las obras de dibujo, pintura, escultura, arquitectura, modelos y obras de arte o ciencia aplicadas al comercio o a la industria, los impresos, planos y mapas, los plásticos, fotografías, grabados y fonogramas.

En cuanto a las ideas, sostiene la libertad de expresión. Por lo tanto, la protección de la propiedad intelectual protege sólo las ideas que están expresadas en algunas de las formas

indicadas con anterioridad. “La protección del derecho de autor abarcará la expresión de ideas, procedimientos, métodos de operación y conceptos matemáticos pero no esas ideas, procedimientos, métodos y conceptos en sí” (Ley N° 11723, 1933, artículo 1).

El Régimen de la Propiedad Intelectual define que el autor tiene la facultad de disponer de sus obras científicas, literarias, artísticas o didácticas. Puede, de tal modo, publicarla, ejecutarla, representarla, exponerla en público, enajenarla, traducirla, adaptarla o autorizar su traducción y reproducirla de cualquier manera. En otras palabras, el titular del derecho de propiedad intelectual puede explotar comercialmente su obra o autorizar a otros a hacerlo. Corolario de esas prerrogativas es su derecho de impedir que cualquier persona no autorizada ejerza estos derechos.

La Dirección Nacional del Derecho de Autor se encarga del régimen legal de la propiedad intelectual a través del registro de las obras científicas, literarias, artísticas o didácticas. Aunque no necesariamente el autor debe registrar su obra para protegerla, porque lo están desde el mismo momento de su creación, sin ningún otro requisito. No obstante, el registro de la obra facilita el proceso de comprobación de la autoría y la pertenencia de los derechos sobre esas obras. Por otro lado, el registro de las obras también permite la demostración del momento en que se creó, siendo un factor esencial cuando otra persona sostiene que una obra le pertenece (Portal Oficial del Estado Argentino, s.f.).

Otro punto importante que define la Ley N° 11723 es el alcance de la protección de la propiedad intelectual. En este sentido, protege al autor de la obra, a los colaboradores y a los herederos. También, son titulares de este derecho las personas que tienen el permiso del autor para traducir, adaptar o modificar la obra. Asimismo, las personas físicas o jurídicas que elaboran programas de computación sobre la obra. En este orden, “como lógica consecuencia del avance de la sociedad en materia de tecnología, y la permanente interacción de las

manipulaciones de dichas tecnologías, las cuales pueden ser aplicadas con fines lícitos o no" (Cilleruel, 2006, p.1).

Los delitos informáticos surgen cuando la tecnología no se utiliza con fines lícitos. En el marco de esta ley, se hace referencia a cuando se infringen los derechos de autoría o de propiedad intelectual. En el contexto en que se sanciona la Ley N° 11723 (1933), se buscó subsanar una de las problemáticas usuales como lo era la reproducción ilegal de obras para su venta sin el permiso del autor. (Celli Triunfetti, 2019). La Ley N° 11723 regula la duración de la protección del derecho de propiedad intelectual. Ella se extiende a toda la vida del autor y a un plazo de 70 años para sus herederos, contados desde el primero de enero siguiente a la fecha de su fallecimiento. Para los intérpretes y productores de fonogramas (registros sonoros) el derecho dura 70 años desde la primera publicación. En el caso de las obras fotográficas, 20 años desde la primera publicación, y para las obras cinematográficas, 50 años desde la muerte del último de los colaboradores (Portal Oficial del Estado Argentino, s.f.).

El uso de obras sin permiso del autor se encuentra penado con la prisión. También se puede secuestrar el material que se publicó sin permiso. En este orden, la defraudación incluye a todo aquel que edite, venda o reproduzca por cualquier medio una obra inédita o publicada sin autorización de su autor. Otro caso que se considera, es la falsificación de obras intelectuales, es decir, la edición de una obra ya editada, ostentando falsamente el nombre del editor autorizado al efecto. Finalmente, queda sujeto a pena todo aquel que edite, venda o reproduzca una obra suprimiendo o cambiando el nombre del autor, el título o altere su texto (Ley N° 11723, 1933.)

4.2. Ley N° 25326 de Protección de Datos Personales

La Ley N° 25326 (2000) tiene como objetivo la protección integral de los datos personales que se encuentran en medios públicos y privados que guardan esta información. De

esta manera, se resguardan los datos personales cuando son utilizados sin el consentimiento de la persona titular de esos datos. Aunque, cabe decir que los datos personales comprenden toda la información de una persona, sea física o jurídica, como la identidad, el domicilio, las deudas, de salud o de crédito, entre otros.

De acuerdo a Sain y Azzolin (2017), la ley de protección de datos personales reglamenta el habeas data conforme a lo dispuesto en el artículo 43 de la Constitución Nacional Argentina (1994). A través de la Ley N° 25326 (2000) se garantiza el derecho al acceso, modificación y eliminación de la información de una persona, física o jurídica, según corresponda. También, otorga el derecho a conocer la existencia de archivos, su finalidad y la forma en que se transmiten los datos personales. Además, posibilita la rectificación de la información que consta en los registros, sean públicos o privados.

La autoridad de aplicación de la Ley N° 25326 es la Agencia de Acceso a la Información Pública. Es un ente autárquico que funciona en el ámbito de la Jefatura de Gabinete de Ministros. Dicha Agencia tiene la función de controlar la protección integral de los datos personales almacenados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, públicos o privados, destinados a dar informes. La Agencia debe garantizar el derecho al honor y a la intimidad de las personas y el acceso a la información (Portal Oficial del Estado Argentino, s.f.)..

Los datos personales que protege la Ley N° 25326 (2000) son tan amplios que comprenden la imagen en videos de sistema vigilancia, los datos biométricos y los datos genéticos. La tecnología facilita la comisión de los delitos informáticos relacionados con la información; por ejemplo, el acceso ilegítimo a bases de datos y a todo tipo de información de datos personales mediante dispositivos informáticos e internet (Celli Triunfetti, 2019).

La irrupción masiva de los sistemas electrónicos de comunicación a fines del siglo XX amenaza con nuevos instrumentos para la protección de la intimidad, la identidad y la

privacidad de las personas. Ante estas inminentes amenazas a los derechos de los datos personales, surge la necesidad del establecimiento de normativas contemplativas de estas problemáticas. Cabe decir que la protección de la intimidad históricamente fue garantizada por la Constitución Nacional, el Código Civil y Penal, pero a partir de la Ley N° 25326 surge la particular protección de los datos personales.

En consecuencia, la protección de los datos personales se erige como un nuevo derecho que reviste de importancia junto a la confidencialidad y privacidad. Así, se introdujo como objeto de tutela jurídica que protege la intimidad de una persona más allá de la convención tradicional. En definitiva, garantiza la calidad, intangibilidad y exactitud de la información, su seguridad y la forma en que las organizaciones tratan los datos personales. A su vez, introdujo modificaciones al Código Penal, que fueron ampliadas posteriormente por la Ley N° 26388 (Aime, 2020).

Cabe señalar que la protección de los datos personales se incorporó en el Código Penal mediante los artículos 117 bis y 157 bis. En el primer orden, se pena con prisión a la persona que proporcione información falsa contenida en un archivo de datos personales. Por su parte, el artículo 157 bis pena con prisión a quien acceda ilegítimamente a los bancos de datos personales o proporcione información registrada de modo ilícito.

La actualización de la normativa refleja la respuesta a las necesidades sociales de protección de la intimidad de una persona ante las conductas delictivas que la transgreden. Sin embargo, la creciente digitalización, el uso de internet y de dispositivos informáticos, complejiza constantemente la tarea del legislador que debe proteger los datos personales. De este modo, los medios informáticos ampliaron la comisión de delitos vinculados al acceso a la información personal almacenados en bases de datos y bancos de datos personales. De allí la necesidad de continuar con la adaptación de la legislación a los nuevos desafíos (Sain y Azzolin, 2017).

4.3. Ley N° 26388 de Delitos Informáticos

La Ley N° 26388 (2008) es el resultado de más de una década de propuestas legislativas vinculadas con los delitos informáticos. De allí que sea conocida como ley de delitos informáticos y representa un avance significativo en la materia en Argentina. Se trata de una actualización normativa fundamental que adapta el Código Penal a los avances tecnológicos y las conductas criminales en este ámbito (Figari, 2009). Dicha normativa introduce modificaciones y artículos nuevos en el Código Penal e incorpora conductas delictivas específicas en materia de delitos informáticos, redefine conceptos clásicos y fundamentales al tiempo que los actualiza y adecua al entorno digital. En concreto, incorpora definiciones vinculadas a la informática, como el documento, la firma digital y el documento privado.

> 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 (Ley N° 26388, 2008, artículo 1; Código Penal, artículo 77).

Por lo tanto, el término documento comprende cualquier representación de actos o hechos, independientemente del soporte utilizado, sea digital o papel, entre otros. En cuanto, a la firma, suscripción, instrumento privado y certificado, la novedad es que pueden ser firmados electrónicamente. La incorporación de esta terminología permite adecuar la normativa a los avances de las tecnologías de la información y comunicaciones.

La modificación que tuvo lugar a raíz de la Ley N° 26388 (2008) representa un cambio profundo en la concepción legal de áreas que el avance tecnológico había dejado obsoleto (Palazzi, 2009). Además de los términos mencionados, se debe mencionar que se amplía la

protección de las comunicaciones del Código Penal: “Será reprimido con prisión de seis (6) meses a dos (2) años, el que interrumpiere o entorpeciere la comunicación telegráfica, telefónica o de otra naturaleza o resistiere violentamente el restablecimiento de la comunicación interrumpida” (artículo 197). Además, el citado artículo amplia el delito de violación de la privacidad con la incorporación del correo electrónico y otras formas de comunicación electrónica. En este orden, se amplía el concepto de correspondencia y se sanciona tanto la interceptación como el acceso no autorizado o desvío de comunicaciones. Así, se subraya que las tecnologías facilitan la comisión de actos ilegales que entorpecen o interrumpen las comunicaciones. En la actualidad este concepto se hace extensivo a las comunicaciones que se dan a través de celulares, computadoras y todo otro aparato conectado a internet.

Si bien constitucionalmente se resguarda la privacidad, en el ámbito penal era necesario la tipificación expresa de la intercepción, acceso y desvió de las comunicaciones electrónicas. En relación a este aspecto, se amplía el bien jurídico protegido porque se protege la privacidad de la información personal. En esta línea, se hace referencia a la incorporación de los delitos introducidos por la Ley de Protección de Datos Personales (Cruzado, 2021).

La ley 26388 (2008) plasma actualizaciones que la sociedad requería en base a los avances tecnológicos que ocasionan día a día nuevas figuras delictivas, llenando algunas lagunas legislativas que la jurisprudencia había señalado. En ese orden de ideas se tipifican nuevas conductas delictivas como la ciberpornografía, que penaliza la producción, financiación, comercialización, facilitación o divulgación, por cualquier medio, de pornografía infantil (Pilmayquen Reina, 2013). Otros de los tipos que prevé la Ley N° 26388 (2008) son las estafas y defraudaciones. En este marco, se amplía el delito de estafa con las nuevas formas comisivas y se incluye el engaño de sistemas automatizados. Antes la jurisprudencia no permitía aplicar esta figura a ordenadores o máquinas automatizadas que no contaban con la

intervención de personas. “De esta forma se reconoce que, debido a la informatización, muchos bienes y servicios se encuentran custodiados por computadoras y la manipulación a los fines de obtenerlos indebidamente es una defraudación” (Palazzi, 2016, p,8). Por consiguiente, la modificación del Código Penal permite sancionar conductas donde no hay intervención humana directa. Por ejemplo, la manipulación fraudulenta de cajeros automáticos o sistemas bancarios. De esta manera, se amplían las formas comisivas de la estafa incluyendo el engaño a sistemas automatizados. En función de esta reforma, se busca evitar los planteos jurisprudenciales que impedían aplicar esta figura a los ordenadores o máquinas automatizadas sin intervención de personas.

Por otra parte, la Ley N° 26388 (2008) modifica el delito de daño porque se abarca al daño a bienes intangibles. En este caso, se comprende el borrado de software o de datos almacenados en un ordenador. De esta forma, se hace referencia a un daño que resulta sumamente perjudicial como lo es la destrucción de documentos guardados en soportes tradicionales. Asimismo, se incluye como delito la distribución de programas que tienen el propósito de causar daños, como los virus informáticos (Cruzado, 2021).

La norma que nos ocupa ensancha notablemente la noción de espacio digital amparado penalmente. La actualización del Código Penal a través de ella representa un esfuerzo legislativo que incorpora diversas figuras delictivas y amplía las existentes. No obstante, no se trata de un trabajo que logró introducir una reforma omnicomprensiva. La actualización todavía no es suficiente en el ámbito de investigación de los delitos informáticos. La reforma omite este aspecto, no señala los procedimientos correctos para este tipo de hechos que, por su modalidad, requieren de formas específicas (Pilmayquen Reina, 2013).

Muchos de los nuevos delitos que requieren una respuesta, a veces de fondo y a veces procesal, no tienen una clara recepción en el código penal. Si bien pueden estar

cubiertos por figuras más generales, siempre es necesario entender el nuevo fenómeno y resolverlo con las normas existentes (Palazzi, 2016, p.8).

Cabe señalar que la cuestión probatoria no fue abordada en la Ley N° 26388 (2008) porque se inscribió netamente a la modificación del Código Penal. Sin embargo, resulta necesaria una adecuada reforma procesal penal que facilite la compresión y la investigación de la delincuencia informática. Sin esta complementación, se encuentra incompleta la legislación en la materia que requiere un abordaje exhaustivo. Sobre todo, en materia probatoria porque existen lagunas sobre que pueden y no hacer las fuerzas de seguridad.

La Ley N° 26388 (2008) representa, de tal modo, un hito relevante en la evolución normativa en materia de delitos informáticos, sin que ello importe desconocer que aún quedan importantes desafíos pendientes; así, por ejemplo, la tipificación de delitos no incluidos hasta el momento y su regulación procesal. Esto quiere decir que, Argentina forma parte de un proceso de adecuación legislativa frente a los continuos avances de las tecnologías. Al mismo tiempo, el país debe alinearse con los estándares del derecho internacional sobre delincuencia informática (Celli Triunfetti, 2019).

Uno de los vacíos más notables en la ley es la falta de una tipificación específica para el robo de identidad. Al respecto de la Ley N° 26388 (2008) cabe decir que esta figura se consideró cubierta en la tipificación de la estafa y la falsedad de documentos. Aunque el robo de identidad podría estar comprendido en estos delitos delineados, la complejidad del fenómeno en el entorno digital demanda de un tratamiento más preciso. Es un delito informático que forma parte de las lagunas legislativas y de políticas públicas para la prevención y concientización de los usuarios de internet. Es más, el robo de identidad trasciende los casos individuales, se trata de un delito masivo que puede implicar la sustracción de claves y datos personales a gran escala. Por lo tanto, es un delito grave que afecta la seguridad, la confianza en los entornos digitales y el comercio electrónico. En este sentido, los

métodos de phishing y el uso de nombres de dominio falsos se utilizan para obtener información personal y financiera. Si bien en Argentina el robo de identidad no alcanza la misma dimensión que en otros países, su avance demanda una adecuada regulación. Sobre todo, si se considera que estas conductas son cada vez más frecuentes y que sus perjuicios son de gran magnitud (Palazzi, 2016).

Una parte de la doctrina estima que la Ley 26388 (2008) debería constituirse como un cuerpo legal autónomo del Código Penal. Cabe decir que dicha ley llena un vacío legal, brinda protección jurídica a conductas ilícitas que se proliferan con la utilización de las TIC e internet, pero su incorporación sólo ensancha los artículos vigentes. En este sentido, Tobares Catala y Castro Argüello (2009) sostienen que se trata de un valioso aporte al sistema jurídico, pero debería ser autónomo, con figuras propias y definiciones específicas. En lugar de esto, se centró en ser una ley de modificación, para incorporar, sustituir, modificar y agregar figuras delictivas a las existentes.

También Arocena (2008) coincide en que hubiera sido adecuado abordar la sistemática en una ley específica porque refiere a un bien jurídico novedoso. En efecto, una normativa de esta magnitud requiere de un enfoque especializado como cuerpo legal autónomo. De esta forma, el tratamiento específico le hubiera permitido la incorporación de nuevas figuras. Más allá de esto, la Ley N° 26388 (2008) es un aporte de vital trascendencia porque incorpora una regulación normativa frente a la realidad informática actual.

La Ley N° 26388 (2008) aborda la problemática de los delitos informáticos en respuesta a las lagunas legales en la materia y brinda respuesta a diversas situaciones de hecho frente a a conductas que quedaban en impunidad, que dejaba la sociedad en un estado de indefensión e inseguridad jurídica. Pese a que esta ley generó controversias en la doctrina, lo cierto es que establece las bases legales para enfrentar situaciones que antes no se podían abordar

adecuadamente. O bien, tratar situaciones que requerían interpretar los casos para que encajaran en delitos previamente tipificados.

4.3.1.Interceptación ilícita

A través del artículo 4 de la Ley N° 26388 (2008) se modificó el artículo 153 del Código Penal para adaptarse a los avances tecnológicos en cuanto a la protección de las comunicaciones privadas. De esta manera, establece penas que van desde los 15 días a los 6 meses de prisión para quienes accedan indebidamente a la correspondencia de otra persona. Específicamente, la norma menciona a las comunicaciones electrónicas, cartas, pliego, despacho telegráfico, telefónico o cualquier otro papel privado.

Las acciones que transgreden este derecho van desde el acceso, apropiación, eliminación y desvío del destino de una correspondencia o una comunicación electrónica. También, la interceptación de comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido. La Ley N° 26388 (2008) establece agravantes para los delitos de interceptaciones ilícitas. Por un lado, cuando se cometiera la comunicación o publicación del contenido de una correspondencia o una comunicación electrónica, la pena que se establece va de 1 mes a 1 año. Por otro, si el delito lo comete un funcionario público, en abuso de sus funciones, debe ser penado con la inhabilitación especial por el doble de tiempo de la condena.

En función de esta actualización del Código Penal, quedan contempladas las interceptaciones ilícitas de las comunicaciones en el ámbito de los delitos informáticos. Es decir, se incluyen a las actuales modalidades de comunicación electrónica. Por ejemplo, cuando se accede indebidamente al texto de un mensaje privado de cualquier servicio de mensajería instantánea o de una red social. Aunque, no se especifica que el mensaje debe contener

necesariamente la voz o caracteres alfanuméricos. Por lo tanto, puede ser de todo tipo de signo y gráfico, audio o video (Sain y Azzolin, 2017).

En otras palabras, la interceptación ilícita incluye todo tipo de comunicación, o por lo menos las actualmente conocidas. Ya desde la Ley N° 19798 (1972) de Telecomunicaciones se concibe como “toda transmisión, emisión o recepción de signos, señales, escritos, imágenes, sonidos o informaciones de cualquier naturaleza, por hilo, radioelectricidad, medios ópticos u otros sistemas electromagnéticos" (artículo 2). Por lo tanto, se trata de un concepto amplio de comunicación electrónica tal como también se comprende en la Ley N° 25250 (2001) de Inteligencia Nacional:

> Las comunicaciones telefónicas, postales, de telégrafo o facsímil o cualquier otro sistema de envío de objetos o transmisión de imágenes, voces o paquetes de datos, así como cualquier tipo de información, archivos, registros y/o documentos privados o de entrada o lectura no autorizada o no accesible al público, son inviolables en todo el ámbito de la República Argentina, excepto cuando mediare orden o dispensa judicial en sentido contrario (artículo 5).

También, se subraya que la interceptación ilícita de las comunicaciones privadas requiere de una intencionalidad clara (dolo). Es decir que debe ser cometido de manera indebida, el delito se funda sobre una figura que excluye toda posibilidad de actuar culposo. Por lo que la acción debe realizarse de manera consciente y con el conocimiento de que se está accediendo a una comunicación dirigida a un tercero. “El dolo del autor, a la par del conocimiento de ser una correspondencia dirigida a un tercero, exige la conciencia de que la abre sin derecho” (Palazzi, 2016, p. 11).

4.3.2. Acceso ilegítimo a sistemas informáticos

La Ley N° 26388 (2008) incorporó el artículo 153 bis al Código Penal estableciendo una pena de 15 días a 6 meses a las personas que cometan el delito de acceso ilegítimo a sistemas informáticos, o sea sin la debida. debida autorización o excediendo la que posee. En este caso, el delito versa sobre el acceso indebido a un sistema o dato informático de acceso restringido, siempre que no se trate de un delito más grave. La pena se incrementa entre 1 mes y 1 año de prisión cuando el acceso ilegítimo se realiza en perjuicio de un sistema o datos informáticos de un organismo público estatal, un proveedor de servicios públicos o de servicios financieros.

Esta disposición busca proteger sistemas informáticos que están diseñados para ser privados y accesibles solo con la debida autorización y brindar una tutela penal más eficaz al derecho a la confidencialidad y a la privacidad del titular del sistema y del dato informático. En este punto, se encuentra relacionado con el artículo relativo a las comunicaciones electrónicas. Aunque, en el artículo 153 bis se alude al acceso indebido y no autorizado a un sistema de carácter privado o restringido.

Se trata de delitos informáticos que incluyen el acceso a una casilla de correo electrónico, al perfil de una red social, a una cuenta de mensajería o cualquier otro sistema o dato informático de acceso restringido y no público. También, quedan incluidos en esta figura delictiva los programas espías que se utilizan para recopilar datos personales sin el consentimiento del dueño. Asimismo, se puede contemplar los casos de acceso a un dispositivo privado o restringido de un usuario (Sain y Azzolin, 2017).

El carácter privado o restringido deja en claro la exclusión de todo acceso a redes, sistemas y contenidos de sitios públicos. En esta línea, Altmark y Molina Quiroga (2012) analizan dos situaciones relacionadas a las tecnologías que quedarían por fuera del ámbito de represión de este delito informático: la ethical hacking y la ingeniería inversa. Pese a que su

finalidad no es dañar la privacidad ni cometer actos ilícitos, estas prácticas podrían interpretarse como infracciones. Y aunque son prácticas con matices, plantean desafíos para los sistemas jurídicos porque pueden afectar la protección de la privacidad de los usuarios.

El testeo de seguridad de falencias de redes informáticas, ethical hacking, es una investigación académica, casera o empresarial. Técnicamente puede involucrar el acceso a sistemas restringidos, pero en algunas ocasiones se realiza con el consentimiento de la "víctima" con motivo de su interés en la detección de errores para su subsanación. Por su parte, la ingeniería inversa o reversa pretende la obtención de información técnica a partir de un producto accesible al público. El objetivo es comprender o replicar la composición y funcionamiento de los programas de computación y componentes electrónicos, entre otros.

4.3.3. Revelación de hechos, actuaciones, documentos y datos secretos

A través del artículo 7 de la Ley N° 26388 (2008) se sustituyó el artículo 157 del Código Penal. En este caso, se busca la protección de la intimidad en relación al ámbito de la administración pública. Más precisamente, se enfoca en la tutela del secreto que los funcionarios públicos deben mantener. En caso contrario, la pena es la prisión que va entre 1 mes a 2 años con inhabilitación especial entre 1 o 4 años. Por lo tanto, la conducta reprimida no es la intrusión, siempre que el acceso a hechos, actuaciones, documentos o datos sea legítima en su ámbito de desempeño (Estrella y Godoy Lemos, 2007; Aboso, 2012).

No se trata de cualquier secreto, sino aquel que se establece por ley, que tiene origen y debe mantenerse así dentro del ámbito de la administración pública con excepción de los de carácter político o militar. El rasgo diferencial de la infracción es que los funcionarios públicos revelan, indebidamente, información a terceros que no están autorizados para conocerla. Se trata, de tal modo, de una acción por la cual el funcionario público revela el secreto por fuera del ámbito que le es propio.

El término revelar que se utiliza en el artículo 157 del Código Penal refiere a "descubrir o poner de manifiesto a/ante alguien que no pertenece al círculo de habilitados a conocer hechos, actuaciones, documentos o datos que, por ley, deben ser secretos (media prohibición legal para su divulgación)" (Riquert, 2016, p. 3). La locución "hechos" se refiere a acontecimientos de cualquier naturaleza, tanto humanos como naturales. La noción de actuaciones comprende todo tipo de trámites, expedientes, resoluciones, diligencias o procedimientos que una autoridad emite, tanto judicial como administrativo o legislativo. El término documentos, destaca Fontán Balestra (2002), no se acuña en sentido técnico estricto, por lo que incluye los diversos informes escritos, despachos, comunicaciones, esquemas o planes de organización, incluso aquellos que no lleven fecha ni firma.

4.3.4. Interferencia en los datos o sistemas informáticos

La Ley N° 26388 (2008) incorporó a través del artículo 10 un segundo párrafo al artículo 183 del Código Penal. Se pena con prisión de entre 15 días o 1 año a quien incurra en el delito de interferencia de datos o sistemas informáticos. La normativa que nos ocupa brinda respuestas al vacío legal que existía respecto a la informática y los daños que su uso podría ocasionar. Como se advierte, el denominado daño informático se incorpora al Código Penal mediante esta figura. El ejemplo que más se puede destacar en este sentido, es la distribución de virus a través de la red.

En la incorporación del segundo párrafo al artículo 183 del Código Penal, se distinguen los verbos típicos de alterar, destruir e inutilizar de los que refieren a vender y distribuir. En el primer grupo, se trata de acciones que son consideradas acciones definitivas que no puedan ser reparadas de ningún modo. Es decir que, tras su comisión, no es posible la reparación o restauración del estado anterior a la interferencia de datos o sistemas informáticos. En caso

contrario, se trata de una acción que adquiere el grado de tentativa, cuando se puede revertir o subsanar el daño ocasionado (Sorbo, 2013).

En principio, la problemática en el tratamiento de estos delitos fue que, históricamente, los documentos o programas o datos informáticos no se consideraban como cosas. Desde esta perspectiva, no se podía realizar daños sobre estas cosas por tratarse de bienes intangibles. No obstante, con la actualización que implicó la ley de delitos informáticos, se amplió el concepto de daños con la inclusión de los datos o programas de un dispositivo electrónico.

De este modo, el espectro de daños se extendió a cualquier medio digital que pueda almacenar información, archivos o programas sin excepciones ni distinción de soportes, siempre que se distinga entre el concepto daño y de la propiedad intelectual de las obras afectadas. La idea del daño informático es amparar los datos y el software de un ordenador, no a la propiedad intelectual como tal, sino al patrimonio. Al respecto, cabe recordar que la protección de la propiedad intelectual cuenta con su propia normativa, como ya se abordó en otro apartado.

Los verbos típicos vender y distribuir hacen referencia a la facilitación de virus o programas con el objeto de causar daños informáticos. A través del artículo 183 del Código Penal se sanciona a quienes los vendan o distribuyan. Por lo tanto, se excluye a aquellos que simplemente los tengan en su poder, salvo que exista una intención de usarlos para dañar programas, datos o sistemas informáticos. El bien jurídico protegido, indudablemente es la propiedad o patrimonio. Además, para que sea caratulado como delito se requiere de la intención específica de causar daño (Palazzi, 2016).

Otro artículo relativo a la interferencia en los sistemas informáticos es el agravante que se incorporó a través del artículo 11 de la Ley N° 26388 (2008). A partir de lo cual, el artículo 184 del Código Penal se refiere a los daños en sistemas informáticos destinados a la prestación de servicios públicos. Así, por ejemplo, el artículo menciona a los servicios de salud, de

comunicaciones, energía, de transporte. En este caso, la pena se sitúa entre los 3 meses y los 4 años y responde a la necesidad de proteger estos sistemas informáticos esenciales para la sociedad que puede verse afectada ante un ciberataque masivo.

La sanción a todo aquel que ejecute este daño va más allá del perjuicio al bien jurídico tutelado de la propiedad de los sistemas informáticos. Por lo tanto, se destaca esta incorporación porque contempla un grave vacío legal al sancionar a quien perjudica potencialmente a la población en su conjunto cuando afecta a un servicio público. Esta es la diferencia respecto de la figura del artículo anterior que también aborda los daños a los sistemas informáticos. “El Legislador, al entender que existe un mayor grado de culpabilidad, optó por agravar el daño informático, cuando éste se ejecuta en sistemas informáticos destinados a la prestación de servicios de salud” (Lucero y Kohen, 2011, p. 145).

Existe una discusión doctrinaria sobre si este agravante de la pena contempla o no al daño que un virus informático puede ocasionar. En este sentido, Palazzi (2016) interpreta que el artículo 184 del Código Penal comprende a los sistemas informáticos y, en consecuencia, a los datos o programas que el ordenador contiene. El fundamento del autor es que el daño afecta a estos elementos, si bien la redacción no los incluye explícitamente. Es decir, en un ciberataque lo que se afecta realmente es el software y los datos, resulta más difícil afectar directamente el hardware de un equipo. Sorbo (2013) agrega una cuestión más al debate al cotejar casos extremos de ataques cibernéticos que exceden el agravante de la pena según el artículo 184 y sostiene que no se contemplan los daños a los sistemas informáticos podrían ser gravísimos para la sociedad al punto de poner en riesgo la seguridad nacional. Por lo tanto, el autor señala que en la reforma del Código Penal no se plantean los ataques informáticos de esta naturaleza, lo que podría ser un desafío en el futuro.

4.3.5. Interrupción de comunicaciones

A través del artículo 12 de la Ley N° 26388 (2008) se sustituyó el artículo 197 del Código Penal. En esta disposición se sanciona con prisión de entre 6 meses a 2 años a quien entorpece o interrumpe una comunicación, sea telegráfica, telefónica o de otra naturaleza. Por consiguiente, se trata de la protección de las comunicaciones de diversos tipos, sean públicas o privadas.

En cuanto a los delitos informáticos, puede ejemplificarse su aplicación a los ataques de denegación de servicio. En este caso, se utilizan las computadoras contra un dispositivo o sistema electrónico con el objeto de volver lento u obstruir las comunicaciones. En efecto, el fin último de este ciberataque es la interrupción de las comunicaciones mediadas por ordenadores. Otro ejemplo, es el hackeo de páginas web. En términos generales, se contempla dentro de este tipo delictivo a:

> Cualquier ataque que afecte el software y hardware de un dispositivo utilizado para establecer comunicaciones, como un celular o cualquier factor que altere o impida la comunicación entre personas a través de correo electrónico, comunicaciones de audio por internet, video conferencias y sistemas de mensajería por celular, entre otros (Sain y Azzolin, 2017, p.100).

Justamente, la especificidad del artículo 197 del Código Penal lo distingue del analizado artículo 184. Sin embargo, en este último ya señala a las comunicaciones como un servicio público que sufre daño frente a los ataques informáticos. Sorbo (2013) advierte que la redacción del nuevo artículo debería haber incluido el término comunicación electrónica. Sin embargo, el legislador incorporó una frase de otra naturaleza antes que definirla con precisión en el ámbito de delitos informáticos. O bien, se podría haber distinguido con comunicación a través de medios electrónicos. En efecto, la idea es la comprensión de la comunicación mediante los sistemas y dispositivos informáticos.

Además de sancionar a quien entorpezca o interrumpa la comunicación, se penaliza aquellos casos de resistencia al restablecimiento de la misma. A diferencia de la primera parte del artículo, la conducta de resistencia al restablecimiento de la comunicación interrumpida implica una actitud activa para mantener la interferencia. En este punto, Sorbo (2013) manifiesta que el legislador podría haber considerado este caso como un agravante de la figura principal de interrumpir o entorpecer. El fundamento se basa en que la interrupción inicial ya es un delito, a lo que suma la actitud de persistencia a restablecer la comunicación implica un mayor perjuicio.

En definitiva, tras el entorpecimiento de la comunicación el trasgresor se esfuerza para que la situación se mantenga. Incluso, frente a aquellos que trabajan contra estos impedimentos sucesivos para solucionar el problema. Por lo menos, esta conducta debería ser agravada en las interrupciones de comunicaciones públicas, especialmente en los casos en los cuales se vean afectados los servicios públicos esenciales, porque esta resistencia podría tener consecuencias severas para el funcionamiento de la sociedad.

Es más, el artículo 197 adjetiva la actitud como resistencia violenta al restablecimiento de la comunicación interrumpida. Entonces, si la disposición subraya la violencia ante los intentos de restitución del servicio, debería constituirse como figura. A partir de ello, la normativa debería establecer un aumento en la pena a aplicarse en estos casos. Se debe destacar que se trata siempre de un delito doloso, por lo tanto, no admite el grado de tentativa, ya que el delito se consuma una vez interrumpida la comunicación.

4.3.6. Falsificación Informática

El artículo 1 de la Ley N° 26388 (2008) incorporó los términos documento, firma, suscripción, instrumento privado y certificado en los últimos párrafos del artículo 77 del

Código Penal. La actualización normativa redefine estos conceptos clásicos del derecho adecuándose al entorno digital.

En este apartado, el análisis será en relación con la Ley N° 25506 de Firma Digital (2001), en donde se define al documento digital como “la representación digital de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo” (artículo 6). Un documento digital proviene de un sistema de elaboración electrónica (Giannantonio, 1987). Por lo tanto, se trata de textos escritos en un procesador de texto, un email, un sitio web, una planilla de cálculo y toda otra información contenida en un soporte electrónico (Portal del Estado, s.f.). En el contexto de la era digital, el avance de la tecnología transformó la manera en que se garantiza la autenticidad y la inalterabilidad de los documentos contenidos en soportes informáticos.

Los documentos electrónicos adquirieron valor jurídico probatorio con la sanción de la Ley N° 25506 y la Ley N° 26388, que la complementa. En estas normativas, se reconoce que la firma digital es un mecanismo válido de suscripción de documentos, otorgándoles validez legal bajo ciertas condiciones.

> Una firma digital es válida si cumple con los siguientes requisitos: a) Haber sido creada durante el período de vigencia del certificado digital válido del firmante; b) Ser debidamente verificada por la referencia a los datos de verificación de firma digital indicados en dicho certificado según el procedimiento de verificación correspondiente; c) Que dicho certificado haya sido emitido o reconocido, según el artículo 16 de la presente, por un certificador licenciado (Ley N° 25506, 2001, artículo 9).

En la Ley N° 26388 (2008) se acuñó el término firma digital. En cambio, en la Ley N° 25506 (2001) este concepto es distinto al de firma electrónica. “Se entiende por firma digital al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto

control" (artículo 2). Se presume que el documento suscrito mediante firma digital no se modificó desde ese momento (Matarasso, 2001).

La Ley N° 25506 (2001) define a la firma electrónica como el "conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales para ser considerada firma digital" (artículo 5). La firma electrónica no tiene el mismo valor probatorio que la firma digital. Por tal motivo, si niegan o desconocen una firma electrónica, el firmante deberá probar que es auténtica. Tratándose de firma digital, en cambio, quien la niega debe probar su falsedad (Portal del Estado, s.f.).

La Ley N° 25506 (2001) conceptúa normativamente al certificado digital como "el documento digital firmado digitalmente por un certificador, que vincula los datos de verificación de firma a su titular" (artículo 13). El certificado digital brinda autenticidad de la identidad y asegura la integridad del mensaje enviado por medios electrónicos, garantizando, de tal modo, que el contenido original no ha sido alterado. Desde el punto de vista probatorio, los peritos informáticos cumplen un papel de vital importancia, porque porque su labor consiste en verificar posibles irregularidades, modificaciones o violaciones efectuadas al correo o documento electrónico.

En relación con la modificación del artículo 77 debe señalarse la derogación del artículo 78 bis y del inciso 1° del artículo 117 bis del Código Penal, según el artículo 15 de la Ley N° 26388 (2008). Para ilustrar mejor esta actualización, cabe recordar el contenido precedente a la reforma. Así, en el artículo 78 bis definía los términos firma y suscripción, que comprenden la firma digital. Por su parte, el inciso 1 del art. 117 bis establecía la pena de prisión a quien inserte o hiciere insertar datos falsos en un archivo de datos personales.

Por lo tanto, en consideración de los últimos párrafos del artículo 77 del Código Penal, se observan los conceptos de los artículos derogados. Es decir, se define al documento, la firma,

la suscripción, el instrumento privado y el certificado. En este sentido, el común denominador es la referencia al término digital, sea expresa o tácitamente. Por lo tanto, de no haberse derogado los artículos 78 bis e inciso 1° del artículo 117 bis, el Código Penal hubiese sido redundante definiendo los mismos términos en artículos diferentes (Sorbo, 2013).

4.3.7. Fraude informático

El artículo 9 de la Ley N° 26388 (2008) incorporó el inciso 16 al artículo 173 del Código Penal, tipificando una nueva figura que versa sobre el delito de estafa o fraude informático. La conducta punible es la cometida mediante cualquier técnica de manipulación que altere el normal funcionamiento de un sistema informático o la transmisión de datos. En este marco, cabe mencionar como antecedente normativo la Ley N° 25930 (2004) que incorporó la defraudación mediante el uso de tarjetas de crédito o débito.

En el Código Penal el fraude informático es una figura que abarca todas las modalidades de estafa o engaño en el marco de los ciberdelitos. De acuerdo a Sorbo (2013) la incorporación de esta tipología provocó grandes debates parlamentarios en torno a dos posicionamientos. Por un lado, se encontraban los legisladores a favor de encuadrar la apropiación de bienes informáticos en la figura de defraudación a través de medios informáticos. Por otra parte, se situaban aquellos que consideraban que dicha apropiación debería ser caratulada como hurto a través de medios informáticos.

La defraudación mediante manipulación informática es una extensión de los delitos contra el patrimonio y/o a la propiedad. Entonces, es similar a la estafa adaptándose a las realidades tecnológicas actuales. Para Lucero y Kohen (2011) el bien jurídico protegido es el patrimonio porque la conducta ilícita lo afecta holísticamente. No se trata de un componente de la propiedad del sujeto damnificado como lo es en el caso de los delitos de hurto o robo.

Palazzi (2016) sostiene que el fraude informático es una nueva modalidad de estafa que implica un perjuicio patrimonial para la víctima y un beneficio económico para el delincuente.

Por lo general la comisión de este delito requiere de conocimientos avanzados en sistemas informáticos. Es decir, que quien comete fraude informático aplica conocimientos específicos para poder manipular los sistemas o una transmisión de datos. Otro elemento primordial es el engaño a la víctima a través de algún tipo de ardid que lleve a cometer un error en favor del perpetrador. Existen múltiples modalidades de fraude informático, como la alteración de registros informáticos, el uso no autorizado de tarjetas de crédito o débito o utilización de claves falsas.

También califica como defraudación la sustracción de datos personales para realizar compras a través de la red, el uso de caballo de troya o técnicas del salami, ya explicados en otros capítulos. Ahora bien, el robo de identidad es un delito que está creciendo exponencialmente entre los delitos informáticos. A través de esta modalidad, el delincuente sustrae y utiliza ilícitamente los datos personales de una víctima para cometer fraudes.

Una característica particular del robo de identidad es que los mismos damnificados proporcionan esta información a través de un engaño. Por ejemplo, encuestas fraudulentas, llamados telefónicos o correos electrónicos falsos que solicitan o verifican datos bancarios, o bien sorteos falsos. También, puede ser a partir del hurto o robo de documentos y tarjetas de crédito o débito, así como cualquier credencial o identificación personal. Otra peculiaridad, es que la víctima del robo de su identidad se percata recién cuando recibe intimaciones para cancelar deudas o juicios ejecutivos y hasta pedidos de detención (Zarate y Becerra, 2011).

> Quien intente robar una identidad puede usar luego la información recolectada para solicitar un crédito o realizar alguna gestión ante un organismo público. Estas acciones pueden dañar la reputación y patrimonio de la víctima, además de costar

tiempo y recursos económicos para reparar el daño (Portal Oficial del Estado, s.f., párrafo 2).

4.3.8. Pornografía infantil

El artículo 9 de la Ley N° 26388 (2008) sustituyó al artículo 128 del Código Penal. En esta disposición se establece la tutela específica de los menores de 18 años frente a la difusión de pornografía a través de medios informáticos. En la actualidad, este delito creció exponencialmente a causa del avance de las tecnologías que facilitan la producción, publicación y distribución. Todas estas acciones son reprimidas con la prisión según el citado artículo, comprendiendo actividades sexuales explícitas o representaciones de los genitales menores de edad con fines sexuales.

Además, se sanciona el lucro del material pornográfico y la facilitación de recursos materiales y humanos para su elaboración y comercialización. Asimismo, se contempla como delito la oferta, venta, alquiler y distribución gratuita de este contenido, tanto en soportes físicos como a través de internet. En todos estos casos, la pena se extiende entre los 6 meses o 4 años de prisión. También, se sanciona con 1 mes a 3 años a quien facilite el acceso a espectáculos pornográficos o suministre material pornográfico a menores de catorce de 14 años.

La facilidad con que la red y las tecnologías permiten la circulación del material pornográfico es facilitada por el anonimato que la informática otorga a los delincuentes. A la vez que los sistemas informáticos complican la identificación de los perpetradores, permiten que la actividad delictiva pueda expandirse a niveles globales. De este modo, se forman redes delictivas relacionadas a la pornografía infantil que demanda el incremento de procedimientos judiciales internacionales para su abordaje. El consenso de organismos supranacionales en torno a la necesidad de combatir este delito da cuenta del carácter transnacional que demanda un enfoque coordinado de tratamiento (Altmark y Molina Quiroga, 2012).

4.3.9. Alteración de medios probatorios

A través del artículo 13 de la Ley N° 26388 (2008) se sustituyó el artículo 255 del Código Penal, con la finalidad de incluir conductas delictivas en el ámbito de los medios de prueba, en particular sobre los sistemas y archivos digitales. Se pena con prisión de 1 mes a 4 años a la sustracción, alteración, ocultamiento, destrucción o inutilización de medios probatorios. Además, establece el agravante en caso de que este delito sea cometido por el mismo depositario, a quien se le suma la inhabilitación especial por doble tiempo. No obstante, si el ilícito se comete por imprudencia o negligencia del depositario, se debe aplicar una multa.

De acuerdo a Sorbo (2013), la disposición que protege a los medios de prueba no tuvo muchas modificaciones en esta oportunidad, a excepción de tres novedades muy puntuales. En principio, se destaca la incorporación del verbo alterar, con el propósito de proteger de cualquier tipo de modificación a los sistemas informáticos y la información que contienen. En especial, se busca comprender la manipulación de las pruebas digitales, se reconoce que cualquier alteración, aunque sea parcial, puede afectar la integridad de los medios probatorios.

Otro término que se introduce con la Ley N° 26388 (2008) se relaciona con lo visto en el párrafo anterior, que versa sobre la alteración en todo o en parte. Es decir, que la modificación de todo el contenido o una parte de un archivo, sistema o prueba informática. Ahora bien, un cambio sustancial es el cambio del término culpable por autor en cuanto distingue entre el responsable del hecho ilícito de la actitud de dolo o culpa. La lógica es que es muy distinto ser el autor material de un hecho, que modifica un archivo o una base de datos o sistemas, que ser el culpable del mismo.

Se trata de un delito doloso porque quien altera, sustrae o daña lo hace con conocimiento del carácter probatorio que tienen los elementos custodiados. La figura admite tentativa porque si la alteración es reversible o permite su recuperación, el elemento de prueba

seguiría siendo útil. Asimismo, el artículo 255 del Código Penal agrava este delito cuando la custodia de los elementos de prueba, denominado depositario, comete el hecho. Del mismo modo, se pena con agravamiento si se trató de una conducta ilícita por negligencia. En todo caso, la disposición refuerza la responsabilidad de aquellos encargados de custodiar evidencias.

4.4. Ley N° 26904 de grooming

La Ley N° 26388 (2008) tipificó las nuevas modalidades de ataque generadas por las TIC, pero no abordó el grooming. Esta laguna jurídica fue resuelta por medio de la Ley N° 26904 (2013) que incorporó el artículo 131 al Código Penal. En esta disposición se sanciona con prisión de 6 meses a 4 años a quien contacta a menores de edad con fines sexuales (Aboso, 2014). Más precisamente, refiere al contacto por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos. A través de esta acción, el propósito del perpetrador es cometer un delito contra la integridad sexual de la persona menor de 18 años.

El artículo 131 incorporó al título de delitos contra la integridad sexual del Código Penal y plasma un evidente avance legislativo, sumamente importante, en materia de delitos informáticos. El grooming es un delito que ocurre cuando una persona adulta acosa a una niña, niño o adolescente para cometer delitos sexuales. Ahora bien, se trata de una figura nueva en tanto que el énfasis normativo señala el contacto o comunicación que se establece por medios electrónicos. Pero, más allá de esta particularidad, es la conducta ilícita de los pedófilos que buscan socavar moral, emocional o psicológicamente al menor de edad con el objetivo de controlarle y consumar el acoso y/o abuso sexual (Celli Triunfetti, 2019).

Justamente, se entiende que el grooming es la acción de captar y manipular a menores de edad a través de medios electrónicos con propósitos sexuales. Es decir, es un proceso dirigido por una persona adulta que busca ganarse la confianza de un menor de edad. El

contacto puede establecerse por diversas vías a través de internet, como chats, redes sociales, juegos o aplicaciones. Asimismo, otra característica específica del grooming es que, para lograr su cometido, la persona adulta simula ser otro menor, como parte del engaño (Sain, 2018).

> Se llama grooming al conjunto de estrategias que una persona adulta realiza para ganarse la confianza de un niño, niña o adolescente, a través del uso de las tecnologías de la comunicación e información, con el propósito de abusar o explotar sexualmente de él o ella. El adulto suele crear un perfil falso en una red social, foro, sala de chat u otro, se hace pasar por un chico o una chica y entablan una relación de amistad y confianza con el niño o niña con la intención de acosarlo
>
> (Oficina de las Naciones Unidas contra la Droga y el Delito, s.f. ,p. 5).

El adulto recurre a diversas técnicas en la comisión del grooming. Por ejemplo, la creación de un perfil electrónico falso para engañar a niñas, niños y adolescentes. El perfil electrónico es una identidad falsa en las redes sociales, sitios de mensajería instantánea o juegos. La falsedad de este perfil en línea va desde el nombre y la edad de la persona adulta que finge ser un menor de edad, hasta el lugar de residencia, entre otros datos (Ministerio de Justicia y Derechos Humanos, 2021).

A través del grooming el delito contra la integridad sexual puede ser un acto preparatorio de una conducta de abuso sexual físico. En este sentido, el artículo 131 del Código Penal prevé la acción de contactar a un menor mediante alguna TIC con propósitos sexuales. Por eso, Vaninetti (2013) sostiene que el grooming “es una etapa virtual previa al abuso sexual en el mundo real” (p. 1). Tazza (2014) manifiesta que el verbo contactar evidencia que la conducta típica es entablar una conexión personal a través de cualquier medio de comunicación, descartando el contacto directo o personal.

El grooming introduce una figura dolosa porque tiene un elemento ultraintencional: la comisión de un delito contra la integridad sexual del menor de edad. En esta línea, resulta difícil

la acreditación de finalidades. No obstante, los medios electrónicos pueden facilitar la explicitación de pruebas con la evidencia del intercambio de audio, video e imágenes entre la persona adulta y el menor. En cuanto a la consumación de la conducta punible, se consuma cuando se establece el contacto en donde sea posible dilucidar el propósito ilícito de la comunicación (Morabito, 2010).

Riquert (2017) alude sobre la dificultad que implica identificar un caso de grooming porque es un proceso que tiene lugar en un lapso temporal prolongado. Es decir, se inicia con el contacto, luego viene la etapa de establecimiento del vínculo afectivo o emocional que permita dar lugar a una relación de confianza. Recién allí, el perpetrador avanza hacia la finalidad prohibida. De esta manera, afirma, sería posible la tentativa de grooming cuando no se consume dicha finalidad por interrumpirse el proceso. Por ejemplo, dado que un control parental de interceptación de mensajes descubre el potencial caso de grooming.

También es viable que, durante el proceso de contacto con intenciones de atentar contra la integridad sexual, se plasmen otras tipicidades concurrentes. Por ejemplo, facilitación de material pornográfico al menor o las exhibiciones obscenas reguladas en los artículos 128 y 129 del Código Penal. La integridad sexual del menor puede verse afectada de forma amplia a través del grooming porque:

> Mediante el engaño y la extorsión se aprovecha de la vulnerabilidad de los menores para diferentes fines, entre los que puede incluir el abuso o la violación en un posterior encuentro con la víctima o la inducción para que el niño, niña o adolescente se desnude frente a la webcam para producir material de contenido sexual para consumo personal y/o distribución o venta en la dark web -redes ocultas y encriptadas de internet (Sain, 2018, p.1).

4.5. Ley N° 27436

La Ley N° 27436 (2018) sustituyó el artículo 128 del Código Penal que se analizó en el apartado sobre la Ley N° 26388 (2008). En líneas generales, se trata de una modificación del lapso de las penas y se introduce un agravante. En el primer párrafo se aumentó la pena de prisión de 3 a 6 años para la producción, financiamiento, ofrecimiento, comercialización, publicación, facilitación o distribución de pornografía de menores de 18 años. En la reforma anterior, esta conducta ilícita se reprimía con prisión de entre 6 meses y 4 años.

El segundo párrafo del artículo 128 reduce la pena de prisión a 4 meses a 1 año y se criminaliza la simple tenencia de material pornográfico. Cabe recordar que en la Ley N° 26388 (2008) se penaliza la posesión de representaciones sexuales explícitas en los casos de que la finalidad sea la distribución o comercialización. En el tercer párrafo del artículo 128 del Código Penal se conserva su texto sin ninguna reforma. En este marco, la novedad legislativa se encuentra en el agregado del último párrafo que introduce un agravante en los casos que la víctima es menor de 13 años. Por lo cual, todas las escalas penales previstas en este delito se deben elevar en un tercio en su mínimo y en su máximo (Figari, 2019).

4.6. Ley N° 27411 de Aprobación de la Convenio sobre Ciberdelincuencia (Convención de Budapest)

En el análisis sobre el avance legislativo a nivel nacional en materia de ciberdelincuencia cabe destacar la sanción de la Ley N° 27411 (2017). A partir de esta normativa, se aprobó el Convenio sobre ciberdelito del Consejo de Europa, que se adoptó en la Ciudad de Budapest en 2001. En este apartado, no se va a profundizar en el instrumento internacional porque ya fue desarrollado en el capítulo correspondiente. Ahora bien, se destaca que la adhesión de Argentina al Convenio de Budapest reafirmó la política criminal sobre la punición de la criminalidad informática.

Aunque la sanción de la Ley N° 27411 tuvo lugar recién en el año 2017, el Convenio de Budapest tiene influencia en Argentina desde la aprobación de la Ley N° 26388 (2008). La tendencia a dedicar esfuerzos en materia de abordaje de delitos informáticos se manifiesta desde entonces. En este marco, cabe mencionar que la Resolución Conjunta N° 866 (2011) y N° 1500 (2011) crea la Comisión Técnica Asesora de Cibercrimen en Argentina. Así, este es un ejemplo de política pública que demuestra el compromiso de la Nación respecto al cibercrimen en el plano internacional (Hertler, 2024).

La recepción del Convenio de Budapest en Argentina tuvo una gran importancia en sus aspectos sustanciales. Es decir, en la tipificación de conductas disvaliosas relacionadas con los delitos informáticos. Asimismo, se adoptó el Segundo Protocolo Adicional al Convenio de Budapest. Vale señalar que la Delegación Argentina afirmó que "para prevenir y perseguir el delito cibernético es fundamental contar con mecanismos e instrumentos adecuados que permitan y faciliten la cooperación y asistencia internacional" (Ministerio de Justicia, 2021, párrafo 6).

La recepción del Convenio de Budapest en Argentina no tuvo el mismo impacto en el ámbito procesal que en los aspectos sustanciales. La adecuación de las normativas en el ámbito procesal no tuvo el mismo avance. En este sentido, el desafío es que se conservó la aplicación analógica de ciertos institutos tradicionales, que no se ajusta acabadamente a la sociedad digital. Por ejemplo, los registros y allanamientos, la interceptación postal y telefónica, entre otros.

Otra crítica doctrinaria que se ha formulado a dicha normativa es que las medidas procesales se deberían evaluar a la luz de las garantías constitucionales que marcan un límite a la intrusión estatal. Ello por cuanto la rapidez de la evolución de la tecnología facilita la trasgresión de la privacidad e intimidad por medios informáticos. Pero, al mismo tiempo, con

la pretensión de proteger estos derechos, las personas pueden verse más expuestas a accesos arbitrarios por parte de las autoridades.

> La gran cantidad de información que puede almacenarse o desprenderse de la prueba digital, al accederse a ámbitos de privacidad e intimidad (…) requiere que las reglas procesales impongan a los operadores judiciales una mayor rigurosidad de los controles a fin de autorizar el acceso y/o registro y/o secuestro de las evidencias digitales (Cruzado, 2021, pp. 38-39).

La advertencia sobre el margen de interpretaciones arbitrarias y los potenciales abusos de autoridad fue advertida por la doctrina. La crítica se extiende tanto sobre la Ley N° 27411 (2017) como la Ley N° 26388 (2008). Al respecto, la observación es que aumentan la inseguridad jurídica en las actividades de investigación penal en el ámbito de los delitos informáticos. El fundamento es que las disposiciones de estas normativas son abiertas y genéricas. De este modo, la amplitud y ambigüedad puso en tela de discusión los riesgos colaterales que pueden suponer para las actividades de investigación en seguridad informática en Argentina (Schulkin, 2018).

Por último, se debe subrayar que el ordenamiento jurídico argentino adhirió al Convenio de Budapest con ciertas reservas que representan un potencial conflicto con la legislación nacional. En general, las reservas son sobre seis disposiciones asociadas a las cuestiones jurisdiccionales y a la pornografía infantil. La reserva sobre el artículo 6.1.b. del Convenio de Budapest que se refiere a la posesión de dispositivos electrónicos, contraseñas o claves de acceso para cometer delitos informáticos. Por ejemplo, el acceso ilícito o los ataques a la seguridad de sistemas informáticos.

> La República Argentina hace reserva del artículo 6.1.b. del Convenio sobre ciberdelito y manifiesta que no regirá en su jurisdicción por entender que prevé un supuesto de anticipación de la pena mediante la tipificación de actos preparatorios, ajeno a su

tradición legislativa en materia jurídico penal (Ley N° 27411, 2017, artículo 2 inciso a).

Las reservas a los artículos 9.1.d., 9.2.b. y 9.2.c. del Convenio de Budapest se fundamentan en que los delitos que regulan son supuestos que resultan incompatibles con el Código Penal. El mismo argumento se establece respecto de la reserva del artículo 9.1.e. del Convenio de Budapest. No obstante, se determina que esta disposición rige de manera parcial porque en Argentina se sanciona la tenencia de pornografía infantil cuanto tiene fines inequívocos de distribución o comercialización. No obstante, con la sanción posterior de la Ley N° 27436 (2018) se penaliza la simple tenencia de este material.

En materia de jurisdicción, se hace reserva a los artículos 22.1.d. y 29.4 del Convenio de Budapest. Al respecto, la Ley N° 27411 (2017) afirma que "su contenido difiere de las reglas que rigen la definición de la competencia penal nacional" (artículo 2 inciso d). Por lo que se refiere a la reserva del artículo 29.4 del Convenio de Budapest, la Ley N° 27411 (2017) sostiene que el requisito de la doble incriminación es una de las bases primordiales de la Ley N° 24.767 de Cooperación Internacional en Materia Penal (1996).

La reserva del artículo 29.4 del Convenio de Budapest señala la conservación rápida de datos informáticos almacenados para una investigación. En este marco, es relevante la regulación de la doble jurisdicción o doble tipificación para la asistencia mutua en un delito informático transnacional. Así, en estos casos se hace reserva del derecho a prestarla cuando un Estado esté convencido de que, al revelar los datos, no se respetará la doble tipificación (Cruzado, 2021).

Si bien el aporte del Convenio de Budapest es sustancial en el ámbito de cooperación internacional en materia penal, cabe señalar una observación que realiza Martins dos Santos (2022). No es un hecho menor considerar que este instrumento tiene origen en un sistema jurídico y político distinto al vigente en los países latinoamericanos. Por lo tanto, un desafío

que se presenta en la región es el proceso de adaptación de acuerdo a los estándares del sistema interamericano. En este sentido, la adhesión en Estados como Chile, Brasil, Argentina, Colombia y México se asemejan en cuanto a:

- La falta de participación de los sectores primordialmente implicados.
- La celeridad en la discusión de las leyes y decretos promulgados sin transparencia y con apuro.
- La utilización de la necesidad de adecuación al Convenio de Budapest para promover reformas integrales de la legislación penal y procesal penal. A partir de lo cual, se pone en riesgo derechos de los ciudadanos, como a la intimidad, la protección de datos y el debido proceso legal.

4.7. Ley N° 27590

Ley N° 27.590 (2020) creó el Programa Nacional de Prevención y Concientización del Grooming o Ciberacoso contra Niñas, Niños y Adolescentes con el objeto de "prevenir, sensibilizar y generar conciencia en la población sobre la problemática del grooming o ciberacoso a través del uso responsable de las Tecnologías de la Información y la Comunicación (TICs) y de la capacitación de la comunidad educativa" (artículo 2). Se trata, de tal modo, de una legislación que profundiza el camino iniciado por la Ley N° 26388 de Grooming (2008).

Tal como se puede advertir, la particularidad de la Ley N° 27.590 (2020) es el esfuerzo por prevenir, sensibilizar y generar conciencia sobre el problema del grooming o ciberacoso. Por ello, se establece como política pública de Estado que se materializa mediante crea el Programa Nacional de Prevención, que se reglamentó con el Decreto N° 407 (2022) (Biblioteca del Congreso de la Nación, 2022). Los objetivos son:

- Generar conciencia sobre el uso responsable de las TIC.

- Garantizar la protección de los derechos de las niñas, niños y adolescentes frente al ciberacoso o grooming.
- Capacitar a la comunidad educativa en el nivel inicial, primario y secundario, tanto de gestión pública como privada, para concientizar sobre el ciberacoso.
- Diseñar y desarrollar campañas de difusión a través de los medios de comunicación.
- Brindar información sobre la forma de denunciar los delitos de ciberacoso en la justicia.

De acuerdo al Portal Oficial del Estado (s.f.) las características principales de la implementación del Programa Nacional de Prevención y Concientización son la segmentación y la accesibilidad. El primer aspecto hace referencia a la adaptación de los materiales de prevención y concientización para que el mensaje llegue de manera más efectiva. Para ello, se debe presentar los materiales de manera diferenciada para cada público destinatario, facilitando su comprensión y que tenga mayor impacto. Los materiales pueden ser recursos digitales, piezas de comunicación, campañas publicitarias, secuencias didácticas, capacitaciones y toda otra herramienta, en soporte papel o digital.

En cuanto a la accesibilidad, se señala la presentación de la información de prevención y concientización en lenguaje sencillo y comprensible para todos. Es decir, se pretende garantizar que todas las personas, sin importar su capacidad o condición, puedan acceder a los contenidos. En este orden, se manda a la adaptación del material y las herramientas con un enfoque inclusivo y efectivo. Por ejemplo, la adecuación de la información mediante intérpretes de Lengua de Señas Argentina o gramática sorda, sistema Braille, audio descripción u otras técnicas pertinentes.

El propósito es la promoción del uso responsable de dispositivos electrónicos, el acceso a internet y a plataformas digitales interactivas. En esta línea, otra estrategia que promueve la Ley N° 27590 (2020) es la inclusión de mensajes digitales de prevención y concientización:

“como pantalla de inicio de teléfonos celulares, teléfonos inteligentes, tablets, y otros dispositivos tecnológicos.” Los mensajes pueden implementarse en los salvapantallas, pantalla de bloqueo, fondo de pantalla o pantalla de actualización del dispositivo. También, en las plataformas digitales como ventana emergente o pauta publicitaria.

4.8. La difusión de contenido íntimo sin consentimiento

En la sociedad hiperconectada por las TIC son muchas las nuevas prácticas digitales que se presentan. Una de ellas, es el envío de contenido íntimo o sexual a través de mensajería instantánea o redes sociales, entre otras posibilidades que la conexión a internet facilita. No obstante, puede constituir un grave riesgo y derivar en otras prácticas digitales peligrosas para la integridad del emisor cuando el receptor lo difunde sin consentimiento. La difusión no consentida de material íntimo es una forma de violencia digital que “consiste en la divulgación, distribución, compilación, comercialización o publicación por cualquier medio de material digital íntimo que retrata, con o sin consentimiento, a una persona mayor de edad que no autorizó su difusión” (Fraga Utges, 2022, p. 5).

En Estados Unidos estos casos acuñaron en la legislación el concepto de pornografía no consentida que es la distribución de imágenes sexuales gráficas de personas sin su consentimiento (Franks, 2016). “Esto incluye tanto las imágenes originalmente obtenidas sin el consentimiento como por ejemplo usando cámaras ocultas, hackeando teléfonos, o grabando abusos sexuales, como así también las imágenes obtenidas en el contexto de una relación íntima” (Curatolo, 2021, p. 5). Por lo tanto, puede ocurrir que la difusión de contenido íntimo no tenga ni el permiso ni el conocimiento de la persona, sobre la existencia de estas imágenes o videos, hasta que se divulga el material.

Además, las TIC tienen la facilidad de difusión masiva ya que el alcance de las redes sociales es muy elevado y rápido a la vez. La exposición de imagen e intimidad del emisor

puede llegar a un número indeterminado de receptores. Por lo tanto, la problemática puede derivar en múltiples daños consecuentes, a tal punto extremo que la víctima tome la decisión de quitarse la vida. El espectro nocivo de la difusión de contenido íntimo sin consentimiento es amplio porque la persona puede sufrir distintas formas de acoso, ciberbullying, chantajes, extorsiones, amenazas, entre otros (Fraga Utges, 2022).

La difusión de contenido íntimo sin consentimiento puede cobrar mucho valor en términos de venganza, factores económicos y de poder. El perjuicio a la integridad es altamente nocivo para la víctima porque puede ser extorsionada, amenazada o coaccionada antes o después de la divulgación de material sexual. De esta forma, el chantaje comprende distintos pedidos, desde dinero en efectivo o depósitos en transferencias, hasta más fotos íntimas.

Este tipo de prácticas puede tener diversas finalidades. Por ejemplo, el perpetrador puede tener la intención de provocar daños a la víctima como una forma de venganza. También, puede ser la obtención de dinero u obligar a la víctima a hacer algo a cambio de no difundir las imágenes o videos íntimos (Portal Oficial del Estado, 2024). En Argentina, esta conducta es considerada como extorsión en el Código Penal, pero no existe una legislación específica vigente sobre la materia.

El problema de vacío legal sobre la difusión de contenido íntimo sin consentimiento dio lugar a distintas iniciativas legislativas. En los últimos años se presentaron diversos proyectos de leyes y de modificación del Código penal argentino, pero ninguno fue aprobado. Por lo tanto, el digesto punitivo carece de una figura en que regule en forma autónoma a los hechos de esta naturaleza. En un mundo que se vuelve cada vez más digital los agresores se apropian del espacio para causar daño mediante la difusión de contenido íntimo sin consentimiento, que se constituye en una grave violencia (Zerda, 2021).

Tal como se analizó en apartados anteriores, la Ley N° 26388 (2008) incorporó disposiciones relativas a los delitos informáticos. Sin embargo, la evolución de las TIC y las

prácticas digitales novedosas continúan su avance y demandan una actualización de la legislación respecto de los ilícitos no contemplados explícitamente. En efecto, el Código Penal tiene respuestas limitadas y no específicas para la difusión de contenido íntimo sin consentimiento. Por ejemplo, sobre la producción y divulgación de material pornográfico de menores de 18 años o la publicación indebida de una comunicación electrónica. O, en el caso de que se cometa un chantaje, se comprende como un tipo de extorsión o a una modalidad de coacción.

Existe un debate doctrinario sobre si la difusión no autorizada de imágenes íntimas debe ser incorporada como delito. En este sentido, el argumento en contra es que la regulación de este tipo de trasgresión iría en contra el principio de mínima intervención penal. La discusión plantea la responsabilidad de la propia víctima por enviar conscientemente imágenes o videos íntimos. Es decir, como acto voluntario de exposición de su intimidad personal a través de material en contexto de sexualidad explícita, tanto en forma individual como con otra/s persona/s.

Desde esta perspectiva, existe una situación de un riesgo asumida libremente. No sólo por la cesión de la materia de contenido sexual, sino por una actitud imprudente. En esta línea, el fundamento es que el emisor depositó en el receptor la confianza de que conservaría en privado dicho contenido. Es decir que esta postura alude que la misma víctima voluntariamente se pone en una situación de vulnerabilidad. Y, que su única garantía es que el receptor respete la privacidad y no divulgue públicamente el material íntimo (Sosa, 2024). En este orden, Martínez Otero (2014) sostiene que el envío del contenido sexual es un acto libre y responsable de exposición de la propia intimidad. Por consiguiente, así como se asume voluntariamente la situación de riesgo se debe atribuir las consecuencias de sus actos. Inclusive cuando los resultados fueron tanto indeseados como previsibles porque la posibilidad de difusión pública era cierta y real desde el mismo momento en que se entregó el contenido explícito. Desde este

enfoque, no es pertinente acudir al derecho cuando esta posibilidad se materializa atentando contra la intimidad.

En contraste, otro sector de la doctrina considera erróneo el argumento del riesgo libremente asumido. Desde este punto de vista, el envío de material íntimo en una comunicación electrónica se contextualiza en el marco de la garantía de secreto entre emisor y receptor. Entonces, el riesgo del envío de la imagen o video con cualquier tipo de contenido no exime de responsabilidad ante la divulgación pública de la intimidad. El riesgo en sí mismo "no constituye un riesgo jurídico penalmente relevante, por lo que no puede existir ningún tipo de imputación a la víctima y por ello el Estado debe intervenir y no permitir que la privacidad de las personas sea vulnerada" (Curatolo, 2021, p. 3). Conforme a esta perspectiva, la doctrina sostiene que no sería contradictoria la intervención estatal para proteger la privacidad de las personas. En definitiva, los funcionarios públicos no se entrometerían en la esfera privada de los ciudadanos porque no revisarían las comunicaciones electrónicas. Más bien, la trasgresión a la intimidad la comete quien difunde material que se produjo en la privacidad. Así, el Estado respondería a los hechos en los casos que la víctima inicie una denuncia.

Vale tener en consideración que el contenido íntimo o sexual puede ser obtenido sin el consentimiento de la víctima. Entonces, no se constituiría como un acto libre, voluntario, consciente y responsable del que se debería asumir las consecuencias no deseadas. Por ejemplo, la persona agredida puede ser retratada sin tener conocimiento durante una práctica sexual. También, se pudo haber obtenido material de desnudez de una persona por fuera del escenario íntimo sexual. Otras prácticas no autorizadas suelen ser las cámaras ocultas en baños, vestidores u otros lugares (Fraga Utges, 2022).

4.8.1. Ley N° 27736 sobre violencia digital

La Ley N° 27736 (2023) establece que la difusión de imágenes íntimas de mujeres sin su consentimiento es una forma de violencia de género. Por eso, es una normativa que modifica la Ley N° 26485 de protección integral a las mujeres (2009) incorporándose como una forma más de violencia entras las ya existentes. Asimismo, la normativa demanda la creación de estrategias y mecanismos de protección, resguardando la seguridad de las víctimas. Principalmente, se propone la promoción de políticas públicas en el ámbito de la educación digital para la prevención de este tipo de agresiones. En forma adicional, se proponen medidas sancionadoras para aquellos que divulguen contenido íntimo sin consentimiento (Buenos Aires CSIRT, 2024).

En este marco, la Ley N° 27736 (2023) agrega al artículo 4 de la Ley N° 26485 (2009) a la violencia contra las mujeres cometidas en el ámbito analógico digital. Este concepto se incorpora como inciso i del artículo 6 de la Ley N° 26485 (2009) como violencia digital o telemática. Así, se la define como toda conducta, acción u omisión en contra de las mujeres basada en su género mediante las TIC con la intención de causarles daños. En esta línea, la normativa contempla de manera integral los aspectos físicos, psicológicos, económicos, sexuales o morales, tanto en el ámbito privado como en el público (Ministerio de las Mujeres, Géneros y Diversidad, 2022).

Se protegen, además, los derechos y bienes digitales, así como el acceso, permanencia y desenvolvimiento de las mujeres en el espacio digital. Por lo tanto, esta forma de violencia incluye todo comportamiento que atente contra la integridad, dignidad, identidad, reputación y libertad de las mujeres. Asimismo, refiere a la producción y difusión sin consentimiento de contenido digital de tipo sexual o de desnudez, es decir, a la trasgresión de la intimidad. Otra conducta reprochable refiere a la divulgación de discursos de odio sexistas, acoso, extorsión,

entre otros. Así como también, el espionaje de la actividad virtual, accesos no autorizados, robo y difusión no consentida de datos personales (Portal Oficial del Estado, 2023).

Se prevé también una serie de medidas cautelares de protección para que las plataformas digitales eliminen los contenidos en línea que generan violencia digital o telemática (Ministerio de Economía, 2023). La autoridad que interviene en estos casos solamente puede efectuar requerimientos necesarios para la investigación. De este modo, puede solicitar a las empresas que revelen los datos relativos al tráfico y al contenido del material suprimido.

Otro aspecto novedoso es que se prohíbe el contacto del agresor hacia la mujer que padece violencia digital. En esta línea, cabe mencionar la modificación del apartado a.2 del artículo 26 de la Ley N° 26485 (2009) que refiere al cese de la intimidación hacia la mujer en el ámbito analógico y digital. Por otra parte, se incorpora el resguardo de la evidencia digital "resguardo diligente y expeditivo de la evidencia en soportes digitales por cuerpos de investigación especializados u organismos públicos correspondientes" (Ley N° 27736, 2023, artículo 9).

4.8.2. Hacia una penalización. Iniciativas legislativas

En el apartado anterior señalamos que la Ley N° 27736 (2023) propicia la prevención, asistencia y acompañamiento a quienes sufrieron violencia digital y que se trata de un avance importante a nivel nacional porque establece un tipo de violencia específico que se comete mediante el uso de las TIC. Se remarca también que dicha normativa busca promover la concientización y educación en perspectiva de evitar estas conductas que transgreden la integridad de las personas en el espacio digital. Sin embargo, no brinda respuestas al vacío legal sobre la difusión del material íntimo sin consentimiento en tanto que no la penaliza.

Actualmente, sólo en la Ciudad Autónoma de Buenos Aires se sanciona la difusión de material íntimo sin autorización como una contravención y con una pena muy tenue. Si bien se

trata de un precedente significativo en la punición con respecto a otras jurisdicciones, sigue sin ser suficiente. La gravedad de la situación es que las personas que fueron afectadas por esta trasgresión no pueden obtener una respuesta inmediata ni específica. El hecho de que no exista una pena para estas conductas impide brindar un abordaje de calidad a las víctimas que se vieron damnificadas en su esfera más privada.

En perspectiva de que el tutelaje integral de la privacidad e intimidad de una persona es sumamente relevante para el sistema jurídico argentino, la difusión de contenido sexual sin consentimiento debe ser enérgicamente sancionada. Su protección real y efectiva no es posible por otras vías menos estigmatizantes, la única opción disponible es la vía punitiva. Tal como se mencionó anteriormente, una parte de la doctrina coincide con esta perspectiva y, sobre todo, aquellos legisladores que presentaron propuestas de leyes al respecto (Sosa, 2024).

En este marco, cabe mencionar los grandes avances legislativos en la materia de algunos países. Por ejemplo, en Estados Unidos está tipificada la pornografía no consentida, es decir, la distribución de imágenes sexuales gráficas que fue o no obtenido con el permiso de una/s persona/s. Si bien no se trata de una norma federal, esta conducta está legislada en la mayoría de los Estados, solamente cuatro de ellos no tienen esta legislación. En Brasil se encuentra penado con prisión de 1 a 5 años en el Código Penal de la siguiente manera:

> El crimen de ofrecer, cambiar, poner a disposición, transmitir, vender o exponerse a la venta, distribución, publicación o divulgación, por cualquier medio, incluso por medio de comunicación masiva o sistema informático, o telemático, fotografía, video u otro registro audiovisual que contenga imagen de violación, o de violación de un vulnerable o que haga apología o induzca a su práctica o, sin el consentimiento de la víctima, escena de sexo, desnudez o pornografía (artículo 218-C).[7]

[7] Traducción del portugués al español de Curatolo (2021)

En España, la tipificación en el Código Penal se incorporó como parte de los delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio en el capítulo sobre la revelación de secretos; así, en el artículo 197 inciso 7 se reprime a quien difunda o ceda a terceros algún contenido sin la autorización de la persona afectada; la pena de prisión va de 3 meses a 1 año, o bien, una multa de 6 a 12 meses ante imágenes o grabaciones audiovisuales obtenidas sin permiso en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros. Además, explicita que la divulgación sin consentimiento que se sanciona es aquella que menoscabe gravemente la intimidad de la víctima.

En Italia, se reprime el envío, entrega, transferencia, publicación o distribución de imágenes o videos de órganos sexuales o contenido sexualmente explícito sin consentimiento. Asimismo, se específica que se comprende a aquel material que se produjo en el marco de la privacidad de la persona representada. La pena es la prisión de 1 a 6 años y una multa que va de 5 mil a 15 mil euros. Igualmente, se sanciona a aquellos que adquirieron dicho contenido y realicen las mismas acciones mencionadas, sin el consentimiento de las personas representadas y para causarles daño, y se establece un agravante en el caso de que el delito lo cometa la pareja o un ex si los hechos se difunden por medios digitales.

La experiencia legislativa, brevemente reseñada, de estos países manifiestan una "tendencia general la tipificación del delito de difusión de imágenes, videos, contenidos sexuales explícitos, desnudez sin el consentimiento de la otra persona" (Curatolo, 2021, p. 7). El proceso de actualización legislativa forma parte de la evolución del uso de las TIC a través del tiempo. En este sentido, la ampliación de las prácticas digitales deviene en nuevas maneras de afectación de los bienes jurídicos tutelados a través de medios informáticos.

Es necesario que la legislación de Argentina evite lagunas jurídicas que no comprendan estos casos. Es importante destacar la existencia de algunos proyectos de ley que se presentaron en los últimos años. Desde el año 2019 al corriente, la Diputada Nacional Mónica Macha

presentó 3 iniciativas sobre penalización de la difusión no consentida de contenidos de desnudez o de carácter sexual.

En el expediente 2987-D-2019 se propuso incorporar el artículo 155 bis al Código Penal. La disposición plantea la sanción de la difusión de dicho material sexual a traición de la confianza en el marco de una relación íntima. El delito refiere a la difusión no consentida de contenidos de desnudez total o parcial o contenido sexual o eróticos obtenidos fruto de una relación íntima. En este orden, se exime a toda persona que difunde este contenido en tanto lo recibe a través de terceros sin relación directa con los participantes retratados en el mismo. También, se indulta de responsabilidad penal a quien obra de este modo con el objetivo inequívoco de proteger un interés público.

La pena de prisión que se proyecta es de 6 meses a 4 años en los casos de difusión por medio de comunicaciones electrónicas, telecomunicaciones, o cualquier otro medio o tecnología de transmisión de datos. Además, se plantea una pena más grave en los casos que el delito tenga concurrencia con los delitos informáticos detallados en el artículo 153. En esta línea, la pena escala a entre 9 meses a 5 cinco años cuando la obtención del material es a través de alguna de las conductas penadas en el artículo 153 del Código Penal de la Nación. Asimismo, se agrava la comisión por parte de un funcionario público, en abuso de sus funciones. En este caso se agrega la inhabilitación especial por el doble del tiempo de la condena.

En el proyecto del año 2019 no se propuso la modificación de los artículos que refieren a la extorsión en el Código Penal. Más precisamente, a la extorsión como método de intimidación o amenaza de difusión de contenidos de desnudez, sexuales o eróticos. El fundamento fue que ya es punible en los términos del artículo 169, si bien con penas menores a las de la extorsión según el artículo 168.

En el 2020 nuevamente se retomaron aspectos del proyecto de ley presentado en 2019. En esta oportunidad, recibió la aprobación en el Senado y fue debatido en la Comisión de Legislación de esta Cámara. La primera diferencia respecto al anterior es que no se propuso la incorporación del artículo 155 bis al Código Penal, sino su modificación. De esta forma, se planteó la conservación de la pena de multa para aquel que publique indebidamente una correspondencia o comunicación electrónica, telegráfica, telefónica o de otra naturaleza. También, se mantuvo la eximición de la persona que actúe de esta manera con el propósito inequívoco de proteger un interés público.

Una distinción respecto del proyecto de ley del 2019, es que se propone la penalización específica de la difusión no autorizada de contenidos de desnudez, sexual o erótico. Asimismo, la conducta ilícita comprende a los casos en que dichos contenidos fueron obtenidos con consentimiento de la víctima. En este orden, se determina que la pena es el doble de la multa mencionada en el párrafo anterior. Además, se establece la de pena de prisión de 3 meses a 3 años cuando dicha conducta transgrede la presunta expectativa de intimidad.

De este modo, tanto la propuesta de incorporación del artículo 155 bis como de la modificación del artículo 155 se enmarcan en el capítulo del Código Penal sobre la violación de secretos y de la privacidad. No obstante, el proyecto de ley que se presentó en el 2020 propone la modificación del artículo 169 que refiere a la extorsión. Por lo tanto, plantea la introducción explícita de la conducta ilícita de difusión de contenido fruto de una relación íntima. Por lo que se refiere al resto de esta disposición, se mantiene igual, con la pena de prisión de 3 a 8 años.

Por lo tanto, la modificación del artículo 169 plantea la difusión de imágenes y videos íntimos como método de extorsión (Sosa, 2024). Por ejemplo, en los casos en que se pide dinero, transferencia, criptomonedas o envió de más imágenes o videos del mismo carácter. Al respecto de la escala penal de esta conducta, Curatolo (2021) manifiesta que sería contrario al

principio de proporcionalidad. En este sentido, sostiene que la pena sería muy elevada en comparación con la posible tipificación del delito de difusión no consentida que va de 3 meses a 3 años de prisión. Por eso, estima que sería más apropiado la sanción de prisión de un 1 a 5 años.

En el proyecto de ley del 2022 se propuso nuevamente la incorporación del artículo 155 bis al Código Penal. Las novedades tuvieron como base el proyecto del 2019 de la Cámara de Diputados y del 2020 aprobado por la Cámara de Senadores. También se tuvo en consideración el dictamen de minoría de la Comisión de Legislación Penal de la Cámara de Diputados del 10/11/2020, el derecho mexicano y español y el Código Contravencional de la Ciudad Autónoma de Buenos Aires.

El proyecto del 2022 pretendía tutelar los siguientes bienes jurídicos: la vida, la integridad física, sexual y psicológica, el derecho a la privacidad, el derecho al honor, el derecho a la intimidad, el derecho a la imagen, la propiedad intelectual de la imagen, y el derecho a vivir una vida libre de violencia. En este marco, se contemplaban como delitos conductas o agravantes no considerados en los proyectos de ley ya analizados; por ejemplo, en la incorporación del artículo 155 bis plantea como delito la obtención de contenido íntimo o sexual sin consentimiento o mediante el engaño de la víctima. En estos casos, la pena de prisión es de 3 meses a 2 años y el doble de la multa que se fija en el artículo 155.

Por lo tanto, en el proyecto del 2022 se busca determinar como delito la videograbación, la audiograbación, la captura de fotografías, la filmación o la elaboración de documentos con contenidos de desnudez, naturaleza sexual o representaciones sexuales explícitas. Por otro lado, se tipifica la difusión, publicación o envío no autorizado de este tipo de material obtenido con o sin consentimiento de la víctima. En este segundo caso, la pena de prisión comprende el doble de multa y la prisión de 3 meses a 3 años. Además, la combinación de dichas conductas,

producción y difusión de contenido íntimo o sexual, se reprime con la prisión de 6 meses a 3 años y el doble de la multa del artículo 155.

Otra novedad del proyecto de ley del 2022 versa sobre la incorporación del artículo 155° ter. Se proponen cinco agravantes de las penas previstas en el artículo 155 bis con el aumento en un tercio de su mínimo y de su máximo. En principio comprende a la persona que esté o haya estado unida a la víctima, sea por matrimonio, unión convivencial o similar relación de afectividad, aún sin convivencia. También, se contempla la comisión con fines de lucro o contra una persona menor de edad. Otro agravante del hecho delictivo es su comisión por placer, codicia, odio racial, religioso, de género o a la orientación sexual, identidad de género o su expresión. Asimismo, considera como agravante la comisión del hecho contra una mujer cuando es perpetrado por un hombre y mediando violencia de género.

El proyecto de ley del 2022 mantiene el espíritu de medicación del artículo 169 del Código Penal que sostiene la propuesta del 2020. No obstante, en esta oportunidad alude a la extorsión de difusión de los documentos referidos en el artículo 155° bis o de documentos que fueren consecuencia de una relación íntima o de violación de secretos. Otra novedad que se propone es la modificación del artículo 72 del Código Penal sobre el ejercicio de las acciones. En este marco, se plantea agregar a las acciones dependientes de instancia privada las que nacen de los delitos previstos en el artículo 155° bis y ter. De similares características, es la modificación que se propone respecto del artículo 73. En esta línea, se añade a las acciones privadas las que nacen del delito de violación de secretos, salvo en los casos de los artículos 154, 155 bis y ter, y 157.

Por lo que se refiere al proyecto de ley del 2024, cabe decir que tiene como base la Ley N° 27736 (2023) y la propuesta que se presentó en el 2022. Una vez más, se plantea la incorporación del artículo 155 bis al Código Penal, aunque con algunos cambios. Por ejemplo, se eleva la pena de prisión en los casos de obtención de contenido íntimo o sexual, por cualquier

medio y sin autorización de la víctima o mediante engaño. En este sentido, la condena que se fija es de 8 meses a 1 año y el doble de la multa del artículo 155.

En el proyecto de ley del 2024 se quita la disposición de reprimir a quien elabore y difunda contenido íntimo o sexual sin consentimiento de la víctima. Por lo tanto, se mantiene la tipificación del delito de difusión, publicación o envío de dichos contenidos. En este aspecto, se conserva la pena de prisión de 3 meses a 3 años y el doble de multa como en el proyecto de ley del 2022. Una novedad es que se pretende penar la difusión de contenido íntimo o sexual que se elaboren mediante las TIC o la inteligencia artificial y no correspondan con la persona que es retratada, señalada y/o identificada en los mismos.

De manera análoga al proyecto de ley del 2022, se propone la incorporación del artículo 155° ter. El texto de esta disposición es el mismo, salvo que en esta ocasión no se incluye el agravante en los casos de comisión contra una persona menor de edad. Ahora bien, la sugerencia de modificación del artículo 169 del Código Penal, sobre extorsión de la difusión de contenido sexual o íntimo sin consentimiento, se mantiene sin novedades en el nuevo texto. También se conserva sin cambios la propuesta de modificación del artículo 72, sobre la acción dependiente de instancia privada que nace del delito de dichos artículos 155 bis y ter.

Finalmente, a diferencia de los proyectos analizados, en 2024 se propone la modificación del artículo 129 sobre delitos contra la integridad sexual. En este sentido, se planea un aumento en la pena de multa de $600.000 a $ 4.000.000 de pesos. La disposición mantiene la sanción de quien ejecuta o hace ejecutar a otros actos de exhibiciones obscenas expuestas a ser vistas involuntariamente por terceros. Pero, en la propuesta de 2024 se agrega como delito las exhibiciones de partes genitales con fines sexuales que se envíen mediante las TIC y la comunicación sin consentimiento de quien las recepta. Por lo demás, se conserva el texto original respecto al agravante en casos de que los afectados sean menores de edad.

CONCLUSIONES

La investigación abordó un análisis teórico-doctrinario y legislativo de los delitos informáticos, tanto a nivel nacional como regional e internacional, en función de los objetivos planteados. El presente estudio permitió abordar de manera integral los delitos informáticos en el ordenamiento jurídico argentino, con especial atención a los problemas teóricos, procesales y probatorios que dificultan su adecuada persecución y sanción, tal como se planteó en el objetivo general. En este marco, se han analizado los principales desafíos que plantea la ciberdelincuencia y se ha constatado que la legislación, si bien ha avanzado en la tipificación de ciertos delitos cometidos en entornos digitales, sigue presentando limitaciones que afectan la efectiva tutela jurisdiccional de los sujetos afectados.

Además, en relación con el primer objetivo específico, se realizó una descripción del avance teórico y doctrinario en materia de delitos informáticos en el primer capítulo, lo que permitió constatar que estos ilícitos han sido objeto de múltiples debates en torno a su conceptualización, clasificación y tratamiento jurídico. Se identificaron características distintivas de la ciberdelincuencia, tales como la transnacionalidad, la instantaneidad, la masividad y el anonimato, elementos que hacen que su abordaje difiera significativamente de los delitos tradicionales. Asimismo, se evidenció que la constante evolución de las tecnologías de la información y la comunicación ha generado un dinamismo que muchas veces supera la capacidad de adaptación del derecho penal. Así, se concluye que no existe una única definición sobre los delitos informáticos. Desde fines del siglo XX, se fueron esbozando diferentes aseveraciones conforme al avance tecnológico y de internet, así como también de la legislación y los presupuestos teóricos y doctrinales en este ámbito. En términos generales, se pudo dilucidar la existencia de algunos elementos en común que permiten una aproximación conceptual del alcance del término.

Se concluyó que los delitos informáticos constituyen conductas ilícitas cometidas mediante TIC, que afectan a personas físicas o jurídicas a través de sistemas informáticos y transmisión de datos electrónicos. Este tipo de delitos se cometen por medios o herramientas informáticas o dispositivos electrónicos, que pueden o no estar conectados a la red de internet. Por lo tanto, los delitos informáticos son conductas ilícitas cometidas mediante las TIC de modo intencional, aisladamente o en serie, contra personas físicas o jurídicas, y que lesionan diferentes valores jurídicos.

Se analizó que algunos autores destacan la relevancia de los conocimientos tecnológicos o específicos en el área para la comisión de los delitos informáticos. Desde esta perspectiva, sólo son cometidos por personas con cierta experticia porque se consideran que son ilícitos muy sofisticados. No obstante, el avance de las tecnologías, el surgimiento de nuevas prácticas digitales y artilugios informáticos refutan que, necesariamente, el sujeto activo del delito sea poseedor de amplios conocimientos informáticos.

Además, se pudo advertir sobre la existencia del debate doctrinario en torno a la definición del bien jurídico protegido en los delitos informáticos. Para algunos autores, simplemente son delitos tradicionales cometidos a través de nuevos medios. Es decir, los bienes jurídicos protegidos son los ya existentes en la estructura tradicional, sólo que se incorporaron medios informáticos o electrónicos de comisión de ilícitos. La segunda corriente afirma la existencia de un nuevo bien jurídico a proteger, pero no están totalmente de acuerdo del tipo que representa. En este sentido, sostienen que la información es el nuevo bien jurídico que demanda la protección para no perder la confianza en el funcionamiento de los sistemas informatizados.

Marcadas estas diferencias teóricas, se pudo observar que la doctrina coincide al respecto de los grandes desafíos que demanda el abordaje de los delitos informáticos en términos de tipificación específica, de investigación, en materia probatoria y procesal.

Primeramente, las dificultades de abordaje se identificaron a partir de la caracterización teórica de los delitos informáticos en el primer capítulo. Luego, en los capítulos posteriores se pudo evidenciar la contrastación en la realidad de estas problemáticas mediante el análisis normativo a nivel internacional, regional y nacional.

El impacto global y la diversidad de bienes jurídicos afectados por los delitos informáticos han obligado a replantear los paradigmas tradicionales del derecho penal. En este sentido, la adaptación del derecho a la realidad actual se ve frustrada por las constantes innovaciones tecnológicas que suelen desarrollarse más rápido de lo que se reforman o implementan las regulaciones de ilícitos al respecto. Por consiguiente, la falta de tipificación específica problematiza la aplicación de la responsabilidad penal por delitos cometidos mediante sistemas informáticos. Asimismo, la dificultad de represión repercute negativamente en la efectiva reparación y tutela jurisdiccional de los sujetos afectados.

Al respecto de los perjuicios o daños de los delitos informáticos, se destaca la diversidad de bienes jurídicos que pueden verse afectados, incluso al mismo tiempo. De esta forma, se refutó la idea que suele tenerse de que los delitos informáticos solamente generan grandes pérdidas económicas para la víctima. Lo mismo en cuanto a la motivación del delincuente. En efecto, se evidenció que los delitos informáticos son pluriofensivos en la medida que pueden afectar la integridad personal en todas sus facetas: el patrimonio, la intimidad, la privacidad, el honor, la reputación o imagen, la vida, la integridad física, sexual y psicológica, la propiedad intelectual y el derecho a vivir una vida libre de violencia.

Otro aspecto que se remarcó es la particular gravedad de los delitos informáticos es que son ilícitos que pueden cometerse haciendo uso de las facilidades y posibilidades de ejecución que proporcionan las TIC. El análisis de las características de los delitos informáticos permite afirmar la complejidad en el tratamiento de este tipo de ilícitos. Las herramientas

propicias para su comisión contrastan con las dificultades de investigación que se vuelven mucho más complejas que las tradicionales.

La transnacionalidad, la instantaneidad y la masividad de los delitos informáticos complejizan su tratamiento en el campo del derecho. Esto significa que el ilícito se puede cometer sin que el ciberdelincuente se encuentre físicamente cerca del sujeto pasivo. También, implica que un ciberataque puede perjudicar instantáneamente y al mismo tiempo a gran cantidad de víctimas. Por lo tanto, las barreras jurisdiccionales no son un obstáculo para su comisión, pero lo es para su investigación. En esta línea, la falta de legislación específica en la materia en los países implicados se suma a la ausencia de una efectiva cooperación internacional en la materia.

Entre estas características nocivas de los delitos informáticos todavía cabe mencionar al anonimato. Las TIC facilitan que los delincuentes puedan ocultar su verdadera identidad o, incluso, sus rastros digitales. Por lo tanto, la investigación se dificulta con la identificación de la autoría del delito. En esta línea, el anonimato puede darse desde un perfil falso en las redes sociales hasta la utilización de la Deep web. Es decir, no siempre se requieren conocimientos ni maniobras delictivas muy sofisticadas para ocultar la identidad del delincuente.

Otro aspecto que complejiza la investigación de delitos informáticos es la volatilidad de la evidencia digital. Por tanto, en el análisis teórico se destacó que este ámbito requiere de una capacitación especial por parte de las autoridades competentes que cumplen estas tareas. Resulta esencial la formación adecuada para lograr la identificación, recolección y preservación de los medios probatorios de la evidencia electrónica. En efecto, la cadena de custodia requiere de una serie de recaudos para asegurar el origen e integridad de la evidencia para que no se pierda, se elimine o modifique. En suma, para la preservación de la fuerza probatoria de la evidencia digital.

De acuerdo a la doctrina, se concluye que uno de los desafíos que se presentan frente a las medidas de investigación que impliquen el uso de las TIC es la intromisión significativa en el derecho a la privacidad. El acceso al contenido de las comunicaciones, la interceptación y el acceso de datos en tiempo real o la utilización de técnicas de investigación remota puede devenir en una trasgresión del derecho de las personas. En esta línea, otro desafío es la necesidad de cooperación entre el sector privado y las fuerzas de seguridad. Es decir, la colaboración en la investigación criminal entre las empresas privadas y/o proveedores de las TIC con las autoridades policiales.

En cuanto al segundo objetivo específico, se llevó a cabo un análisis del marco normativo internacional y regional en materia de delitos informáticos y se ha arribado a algunas conclusiones que se consideran relevantes. En primer lugar, la existencia del consenso respecto de la necesidad de su abordaje coordinado y basado en la cooperación internacional. En este escenario, se destacó que las características particularidades de los delitos informáticos demandan un régimen jurídico internacional que sirva de marco referencial. Sobre todo, para que se garantice la compatibilidad y aplicación adecuada cuando el hecho ilícito exceda los límites jurisdiccionales de los Estados implicados.

Así, se concluye que a nivel mundial los delitos informáticos se constituyen en un reto considerable para los afectados, los legisladores, los agentes encargados de las investigaciones y los funcionarios judiciales. Así, la escala mundial de la problemática demanda un tratamiento que no debe ser aislado. Al contrario, requiere de la cooperación interinstitucional e internacional. En este sentido, Se identificó que organismos como la ONU, la OEA y la Unión Europea han impulsado diversas iniciativas legislativas y acuerdos multilaterales para afrontar la problemática del cibercrimen. Entre ellos, se destacó el Convenio de Budapest sobre Ciberdelincuencia, el cual constituye el principal instrumento internacional en la materia y establece pautas para la armonización legislativa y la cooperación entre Estados. No obstante,

se advirtió que la adhesión a estos tratados no siempre se traduce en una efectiva implementación de sus principios en el ámbito interno de cada país.

Respecto al tercer objetivo específico, se analizó la legislación argentina sobre delitos informáticos, destacando avances como la sanción de la Ley N.º 26388 que incorporó nuevas figuras delictivas en el Código Penal. Sin embargo, se constató que esta normativa resulta insuficiente para abordar fenómenos emergentes como la difusión de contenido íntimo sin consentimiento, el acoso digital y otras formas de violencia en línea. Asimismo, persisten dificultades en la persecución penal de estos delitos debido a la falta de herramientas procesales eficaces, la complejidad en la recolección y preservación de evidencia digital y la escasa cooperación internacional.

En este sentido, la investigación permitió confirmar la hipótesis inicial: la actual legislación penal argentina sobre delitos informáticos presenta serias limitaciones en términos de tipificación, persecución y sanción. La evolución constante de las TIC y el surgimiento de nuevas modalidades delictivas han generado un escenario en el que el marco normativo vigente resulta insuficiente para garantizar una respuesta jurídica efectiva. Además, la falta de adecuación de los procedimientos procesales a las particularidades de los delitos informáticos obstaculiza la obtención de pruebas y la identificación de los responsables, lo que en muchos casos favorece la impunidad.

En Argentina, los intentos de actualización legislativa en materia de delitos informáticos comenzaron en 1996, pero no se materializaron hasta el 2008. Durante ese período, existió un vacío legal que dificultó la persecución de estos delitos y dejó a las víctimas sin una adecuada tutela jurisdiccional. Además, no adecuaba su normativa conforme a los parámetros internacionales y regionales que se venían celebrando desde el siglo pasado. La Ley N° 26388 del 2008 representó un avance significativo, al modificar el Código Penal para incluir delitos informáticos y armonizarlo con normativas sobre protección de datos, propiedad

intelectual y firma digital. Además, redefinió conceptos clave, como documento y firma, adaptándolos a la digitalización, y amplió la protección frente a delitos que afectan la privacidad y la comunicación electrónica.

De esta forma, se subsanaron algunas lagunas legislativas con la introducción de nuevas figuras delictivas, agravantes o la incorporación específica de los delitos que se cometen por medios informáticos. Así, el daño informático brindó respuesta a la problemática de que antes los documentos o programas o datos informáticos no se consideraban como cosas, y desde esta perspectiva no se podía realizar daños sobre estas. Se evidenció que el surgimiento de nuevas conductas sumamente perjudiciales demandaba a la legislación un nuevo tratamiento y sanción que resguarden la seguridad en el espacio digital. Por ejemplo, la protección de la intimidad en relación al ámbito de la administración pública y la tutela específica de los menores de edad frente a la producción y difusión de pornografía a través de medios informáticos.

En cuanto al ámbito de los medios de prueba, se incorporó las conductas delictivas sobre los sistemas y archivos digitales. De este modo se reprime toda alteración, sustracción, ocultamiento o destrucción de los medios probatorios digitales. Además, se establece un agravante en caso de que este delito sea cometido por el mismo depositario, a quien se le suma la inhabilitación especial por doble tiempo. Una aclaración esencial en esta disposición fue que la alteración de los medios de prueba puede ser en su totalidad o en parte. Además, se inscribió como un delito doloso porque quien genera el daño lo hace en conocimiento del carácter probatorio de los elementos custodiados. Así, se refuerza la responsabilidad de aquellos encargados de custodiar evidencias.

Así, la Ley N° 26388 fue un hito importante en la evolución normativa en materia de delitos informáticos, pero se trata de un avance en un proceso lleno de desafíos pendientes. Por ejemplo, la tipificación de delitos no incluidos hasta el momento y su regulación procesal. No se puede negar que esta ley se inscribió netamente a la modificación del Código Penal. Sin

embargo, resulta necesaria una adecuada reforma procesal penal que facilite la compresión y la investigación de la delincuencia informática. Sin esta complementación, se encuentra incompleta la legislación en la materia que demanda un abordaje exhaustivo. Sobre todo, en materia probatoria porque existen lagunas sobre qué pueden y que no pueden hacer las fuerzas de seguridad.

Por otra parte, en el 2013 se sancionó la Ley N° 26904 de grooming que subsanó una laguna jurídica que la ley de delitos informáticos no abordó. En definitiva, su importancia deviene de que se tipificó una de las nuevas modalidades de ataque contra la integridad sexual cometidas por medio de las TIC. Más precisamente, en contra de las personas menores de edad cuando el delincuente los contacta por medios informáticos con fines inequívocamente sexuales. En este orden, la particularidad es este tipo de contacto y la intención con que se realiza puesto que el grooming es la acción de captar y manipular a menores de edad a través de medios electrónicos con propósitos sexuales.

En forma complementaria a la ley de grooming, a través de la Ley N° 27.590 que creó el Programa Nacional de Prevención y Concientización del Ciberacoso contra Niñas, Niños y Adolescentes. De esta forma, en el 2020 la sanción de esta normativa tuvo la particularidad de generar espacios de sensibilización para la protección de los derechos en este ámbito. En este sentido, las disposiciones buscaron promover la educación sobre el grooming a través de la escuela y de campañas a través de las TIC.

Otra normativa relativa a los delitos contra la integridad sexual es la Ley N° 27736 que se sancionó en el 2013. A través de esta, se incorpora la violencia digital a las circunscritas por la Ley N° 26485 de protección integral a las mujeres del 2009. En concreto, el objetivo de la ley es la prevención y la protección de las víctimas de la difusión de imágenes íntimas sin su consentimiento. No obstante, no se establece ninguna medida punitiva, ni se incorpora ninguna tipificación en el Código Penal.

Por su parte, la Ley N° 27436 que sustituyó el artículo 128 del Código Penal que fue modificado por la Ley N° 26388. En esta ocasión, se aumentó el tiempo de las penas de prisión en los casos de producción, financiamiento, ofrecimiento, comercialización, publicación, facilitación o distribución de pornografía de menores de 18 años. Un aspecto importante es que se penaliza la simple tenencia de material pornográfico infantil a diferencia de la modificación anterior. Además, se introduce un agravante en los casos que la víctima es menor de 13 años.

En efecto, aún quedan desafíos pendientes comprensibles en una sociedad que se encuentra inmersa en el mundo digital, los avances tecnológicos y nuevas prácticas informáticas. La evolución de las TIC es tan constante y acelerada que sobrepasa el ritmo en que la adaptación del derecho y la doctrina, productos del consenso social, tienen lugar. La complejidad del fenómeno delictivo en el entorno digital demanda un arduo trabajo al legislador que deben ser acompañados por políticas de Estado para la prevención y concientización.

Desde esta perspectiva y en consideración de la investigación realizada, se concluye que es realmente necesario la penalización de la difusión de contenido íntimo sin consentimiento. La estipulación de esta conducta sumamente perjudicial como una violencia digital fue señalada por la Ley N° 27736. Sin embargo, no se tipificó como una nueva figura punible, por lo que el abordaje resulta inefectivo en cuanto a la tutela de derechos fundamentales de los sujetos afectados por la comisión de este delito. No hay lugar a dudas de que existe voluntad de los legisladores respecto de esta problemática porque durante los últimos años se presentaron varios proyectos de ley, mayormente analizados en la investigación.

Ahora bien, ninguna de estas iniciativas que proponen la modificación del Código Penal fueron aprobadas. El problema de vacío legal sobre la difusión de contenido íntimo sin consentimiento no se resuelve porque no se llega a un consenso legislativo. Es más, en la doctrina existe un debate entre el sector que considera la responsabilidad misma de la víctima

y aquellos que entienden que es una cuestión mucho más compleja. Mientras tanto, los agresores se apropian del espacio digital para causar daño mediante la difusión de contenido íntimo sin consentimiento. Así, importantísimos bienes jurídicos están siendo transgredidos porque se trata de una violencia que afecta íntegramente a la víctima.

Es urgente actualizar y fortalecer el marco normativo argentino sobre ciberdelincuencia. Esto implica no solo la tipificación de nuevas conductas delictivas, sino también la implementación de herramientas procesales efectivas y la capacitación de operadores judiciales para garantizar investigaciones eficaces. Asimismo, se resalta la importancia de fomentar la cooperación internacional y la adopción de estándares globales en la lucha contra el cibercrimen, así como la necesidad de implementar estrategias de prevención y concientización que contribuyan a la protección de los derechos de los ciudadanos en el entorno digital. En definitiva, la investigación evidencia la necesidad de un enfoque integral que combine la actualización del derecho penal con estrategias de prevención, educación y asistencia a las víctimas. Solo así se podrá garantizar una protección efectiva contra los delitos informáticos en la sociedad digital contemporánea.

REFERENCIAS BIBLIOGRÁFICAS

ABOSO, G. E. (2012). *Código Penal de la República Argentina. Comentado, concordado con jurisprudencia*. Buenos Aires: ed. BdeF.

ABOSO, G. E. (2014). El delito de contacto telemático con menores de edad con fines sexuales (child grooming) en el Código Penal argentino. *Revista de Derecho Penal y Criminología*, *4* (2).

ACURIO DEL PINO, S. (2015). *Derecho Penal Informático. Una visión general del Derecho Informático en el Ecuador con énfasis en las infracciones informáticas, la informática forense y la evidencia digital*. Editorial Académica Española.

ACURIO DEL PINO, S. (2016). *Delitos Informáticos: Generalidades.* Ecuador: Pontificia Universidad Católica del Ecuador.

AIME, J. I. (2020). La Protección Penal de los Datos Personales. https://www.redipd.org/sites/default/files/2020-01/Proteccion_penal_de_los_datos_personales.pdf

ALAMILLO DOMINGO, I. (2009). Las políticas públicas en materia de seguridad en la sociedad de la información. *Revista de los Estudios de Derecho y Ciencia Política de la UOC*, 9, 13-24. https://www.raco.cat/index.php/IDP/article/download/220827/301630

ALTMARK, D. R. y MOLINA QUIROGA, E. (2012). *Tratado de derecho informático. Tomo I.* Buenos Aires: La Ley.

AROCENA, G. A. (2012). La regulación de los delitos informáticos en el Código Penal argentino. Introducción a la Ley Nacional núm. 26.388. *Boletín Mexicano de Derecho Comparado*, *45* (135), 945-988. https://www.scielo.org.mx/scielo.php?pid=S0041-86332012000300002&script=sci_abstract

Asociación Internacional de Derecho Penal (2014). *Sociedad de la información y derecho penal*. En XIX Congreso Internacional de Derecho Penal.

ATKINS, T.B. (1998). La cooperación internacional policial en el ciberespacio. En CARRASCOSA LÓPEZ, V. (Coord.). Jornadas Internacionales sobre el Delito Cibernético. *Informática y derecho. Revista iberoamericana de derecho informático*, (27- 29), 277-290. https://dialnet.unirioja.es/descarga/articulo/248168.pdf

ATKINS, T.B. (1998). La cooperación internacional policial en el ciberespacio. Informática y derecho. *Revista iberoamericana de derecho informático, 27, 28 y 29.*

BACIGALUPO SAGGESE, S. (2005). Derecho penal y construcción europea. BACIGALUPO SAGGESE, S. y CANCIO MELIÁ, M. (Coords.). *Derecho penal y política transnacional*. Ed. Atelier.

BENEDITO AGRAMUNT, J. (1998). Hacia la sociedad de la información. En CARRASCOSA LÓPEZ, V. (Coord.). Jornadas Internacionales sobre el Delito Cibernético. *Informática y derecho. Revista iberoamericana de derecho informático*, (27- 29), 233-252. https://dialnet.unirioja.es/descarga/articulo/248158.pdf

BENEDITO AGRAMUNT, J. (1998). Hacia la sociedad de la información" en Informática y derecho. *Revista iberoamericana de derecho informático, 27, 28 y 29.*

Biblioteca del Congreso (2022). *Ciberacoso contra niñas, niños y adolescentes. Grooming.* https://bcn.gob.ar/uploads/adjuntos/Dossier-235-legis-nacional-grooming-agos-2022.pdf

Buenos Aires CSIRT (2024). *Ley Olimpia y Ley Belén: protegiendo los derechos en el ciberespacio.*https://buenosaires.gob.ar/sites/default/files/2024-03/B2_Ley%20Olimpia%20y%20Bel%C3%A9n_0.pdf

BUOMPADRE, J. E. (2017). *Manual de derecho penal. Parte especial*. Buenos Aires: Editorial Astrea.

CALONGE VELÁZQUEZ, A. (2006). Sistema competencial y de fuentes en el espacio de libertad, seguridad y justicia. *Revista de derecho de la Unión Europea*, nº 10, 95-112.

CARRASCO ANDRINO, M.M. (2009). El acceso ilícito a un sistema informático. En ÁLVAREZ GARCÍA, F. J., MANJÓN-CABEZA OLMEDA, A. Y VENTURA PÜSCHEL, A. (Coord.). *La adecuación del derecho penal español al ordenamiento de la Unión Europea. La política criminal europea*, 341-364.

CARRASCOSA LÓPEZ, V. (1998). ¿Es necesaria una legislación mundial para Internet? En CARRASCOSA LÓPEZ, V. (Coord.). Jornadas Internacionales sobre el Delito Cibernético. *Informática y derecho. Revista iberoamericana de derecho informático*, (27- 29), 73-112. https://dialnet.unirioja.es/descarga/articulo/248146.pdf

CARRASCOSA LÓPEZ, V. (1998). ¿Es necesaria una legislación mundial para Internet? Informática y derecho. *Revista iberoamericana de derecho informático, 27, 28 y 29.*

CARRASCOSA LÓPEZ, V. (1998). Jornadas Internacionales sobre el Delito Cibernético" en *Informática y derecho. Revista iberoamericana de derecho informático*, (27- 29).

CASTELLS, M. (2001). *Prólogo: la red y el yo*. En Castells, M. *La era de la información: economía, sociedad y cultura.* México D.F.: Siglo XXI Editores.

CASTILLO JIMÉNEZ, C. (1998). Protección de la intimidad en Internet. *Revista iberoamericana de derecho informático, 27, 28 y 29.*

CATALA, G. H. T. y CASTRO ARGÜELLO, M. J. (2009). *Delitos Informáticos.* Córdoba: Advocatus.

CELLI TRIUNFETTI, S. (2019). *Las nuevas tecnologías y los delitos informáticos. Análisis de la ley 26.388 Modificación del Código Penal argentino.* https://repositorio.21.edu.ar/bitstream/handle/ues21/16861/CELLI%20TRIUNFETTI%20Sebastian.pdf?sequence=1

CHICHARRO LÁZARO, A. (2009). La labor legislativa del Consejo de Europa frente a la utilización de Internet con fines terroristas. *Revista de Internet, derecho y política, 9,* 1-14. https://dialnet.unirioja.es/descarga/articulo/3101795.pdf

CHILLIER, G. Y FREEMAN, L. (2005). El Nuevo Concepto de Seguridad Hemisférica de la OEA: Una Amenaza en Potencia. https://www.wola.org/sites/default/files/downloadable/Regional%20Security/past/El%20nuevo%20concepto%20de%20seguridad_lowres.pdf

CILLERUEL, A. R. (2006). La Ley Nº 11.723: algunas consideraciones desde la dogmática y la práctica jurídica. *Revista de la Asociación de Magistrados y Funcionarios de la Justicia de la Nación, 41.* http://ijeditores.com/articulos.php?idarticulo=48906&print=1

COM(2007)267 final, de 22 de mayo de 2007. Comunicación de la Comisión al Parlamento Europeo, al Consejo y al Comité de las Regiones. Hacia una política general de lucha contra la ciberdelincuencia. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:ES:PDF

COM(2008)448 final, 14 de julio, 2008.

COM(2008)448 final, de 14 de julio de 2008. Informe de la Comisión al Consejo basado en el artículo 12 de la Decisión Marco del Consejo, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información.

COM(2009)149 final, de 30 de marzo de 2009. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Sobre protección de infraestructuras críticas de información. Proteger Europa de ciberataques e interrupciones a gran escala: aumentar la preparación, seguridad y resistencia. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:ES:PDF

COM(2010)245 final/2, 26 de agosto, 2010, “otras acciones” relativas al punto 2.3 “confianza y seguridad”.

COM(2010)245 final/2, de 26 de agosto de 2010. Acciones 6 y 7 relativas al punto 2.3. Confianza y seguridad. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:ES:PDF%3E

COM(2011)163 final, de 31 de marzo de 2011. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Sobre protección de infraestructuras críticas de información. Logros y próximas etapas: hacia la ciberseguridad global. https://www.bizkaia.eus/ogasuna/europa/pdf/documentos/11-com163.pdf?hash=f1a5c4522ce412c4e5cbf21eb5817a48

COM(2012)140 final, 28 de marzo, 2012.

COM(2012)140 final, de 28 de marzo de 2012. Comunicación de la Comisión al Parlamento Europeo. La represión del delito en la era digital: creación de un centro europeo de ciberdelincuencia. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52012DC0140&from=hu

Comisión de las Comunidades Europeas (2001). Comunicación de la Comisión Al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2000:0890:FIN:ES:PDF

Comisión Europea (2010). Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a los ataques contra los sistemas de información, por la que se deroga la Decisión marco 2005/222/JAI del Consejo. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52010PC0517

CONSEJO DE EUROPA (1989). Recomendación N° R(89)9 del Comité de Ministros a los Estados miembros sobre delitos informáticos.

CONSEJO DE EUROPA (8 de febrero de 2024). Adhesión al Convenio sobre la Ciberdelincuencia: Beneficios. https://rm.coe.int/cyber-buda-benefits-8febrero2024-es/1680ae7115

Convenio sobre la Ciberdelincuencia de Budapest, 23 de noviembre, 2001. https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

CORCOY BIDASOLO, M. (2007). Problemática de la persecución penal de los denominados delitos informáticos. *EGUZKILORE*, *21*, 7-32. https://www.ehu.eus/documents/1736829/2176629/01+Corcoy.indd.pdf

CRUZADO, C. (2021). *Los Delitos Informáticos en Argentina a partir de la adhesión al Convenio de Budapest.* **[** Tesis de Maestría en Derecho Penal y Ciencias Penales, Facultad de Derecho, Universidad Nacional de Cuyo]. https://ddhh.bdigital.uncu.edu.ar/objetos_digitales/19737/cruzado-tesis-.pdf).

CURATOLO, S. (2021). La tensión entre la difusión no consentida de contenidos sexuales por medios electrónicos y el principio de mínima intervención penal. *Revista Pensamiento Penal*, *395*. https://www.pensamientopenal.com.ar/system/files/2021/07/doctrina89343.pdf

DAVARA, M. A. (2002). *Fact Book del Comercio Electrónico*. España: Ediciones Arazandi.

DE ESTEBAN ALONSO, J. y GONZÁLEZ-TREVIJANO SÁNCHEZ, P. (2004). *Tratado de Derecho Constitucional II*. Ed. Universidad Complutense Madrid.

DE ESTEBAN ALONSO, J. y GONZÁLEZ-TREVIJANO SÁNCHEZ, P. (2004). *Tratado de Derecho Constitucional II*. Ed. Universidad Complutense Madrid.

DE LA CUESTA ARZAMENDI, J. L. y DE LA MATA BARRANCO, N. J. (2010). *Derecho Penal Informático*. Thomson Reuters.

Decisión 91/242/CEE del Consejo de Ministros, 31 de marzo, 1992.

Declaración de Salvador sobre estrategias amplias ante problemas globales: los sistemas de prevención del delito y justicia penal y su desarrollo en un mundo en evolución, 12 al 19 de abril de 2010. https://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/Salvador_Declaration/Salvador_Declaration_S.pdf

Decreto N° 407 de Reglamentación de la Ley N° 27.590 (2022, 14 de julio). Congreso de la Nación Argentina. Boletín Nacional. https://www.pensamientopenal.com.ar/system/files/Documento_Editado552.pdf

DEL MORAL TORES, A. (2001). El coste del delito informático. *Cuadernos de la Guardia Civil: Revista de seguridad pública, 23*, 85-92.

Deluca, S. y Del Carril, E. (2017). Cooperación internacional en materia penal en el MERCOSUR: el cibercrimen. *Revista de la Secretaría del Tribunal Permanente de Revisión, 5*(10), 13 - 28. http://scielo.iics.una.py/pdf/rstpr/v5n10/2304-7887-rstpr-5-10-00013.pdf

DEVOTO, M. (1998). La economía digital: el dinero electrónico y el lavado de dinero. *Revista iberoamericana de derecho informático, 27, 28 y 29.*

DI IORIO, A. H.. (2017). *El rastro digital del delito: aspectos técnicos, legales y estratégicos de la informática forense*. Universidad FASTA. http://redi.ufasta.edu.ar:8082/jspui/bitstream/123456789/1593/2/El%20Rastro%20Digital%20Delito.pdf

DI LEONE, N. (1998). La cooperación policial internacional en el ciberespacio. *Revista iberoamericana de derecho informático, 27, 28 y 29.*

DÍAZ GARCÍA (s.f.) *El bien jurídico tutelado de la información y los nuevos verbos rectores en los delitos electrónicos*. Universidad Santiago de Cali. Facultad de Derecho.

DÍAZ GÓMEZ, A. (2010). El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest. *Revista Electrónica De Derecho De La Universidad De La Rioja*, *8*, 169-203. https://publicaciones.unirioja.es/ojs/index.php/redur/article/view/4071/3321

DÍAZ GÓMEZ, A. (2010). El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest. *REDUR 8*, 169-203. https://publicaciones.unirioja.es/ojs/index.php/redur/article/view/4071/3321

DOS SANTOS, B. (2022). Convenio de Budapest sobre la Ciberdelincuencia en América Latina: Un breve análisis sobre adhesión e implementación en Argentina, Brasil, Chile, Colombia y México. https://www.derechosdigitales.org/wp-content/uploads/ESP-Ciberdelincuencia-2022.pdf

ESTRADA CORONA, A. (2004). *Protocolos TCP/IP de internet. Revista Digital Universitaria*, *5*(8).

ESTRADA GARAVILLA, M. (s.f.). *Delitos informáticos.* México: Universidad Abierta.

ESTRADA GARAVILLA, M. (s.f.). *Delitos informáticos.* México: Universidad Abierta. https://perso.unifr.ch/derechopenal/assets/files/articulos/a_20080526_32.pdf

ESTRADA POSADA, R. Y SOMELLERA, R. (1998). Delitos informáticos . Informática y derecho: *Revista iberoamericana de derecho informático, 27-29*, 423-442.

ESTRADA POSADA, R. y SOMELLERA, R. (1998). Delitos informáticos. En CARRASCOSA LÓPEZ, V. (Coord.). Jornadas Internacionales sobre el Delito Cibernético. *Informática y derecho. Revista iberoamericana de derecho informático*, (27- 29), 423-442. https://dialnet.unirioja.es/descarga/articulo/248204.pdf

ESTRADA POSADA, R. y SOMELLERA, R. (1998). Delitos informáticos. Informática y derecho. *Revista iberoamericana de derecho informático, 27, 28 y 29.*

ESTRELLA, O. A. y GODOY LEMOS, R. (2007). *Código Penal. Parte Especial. De los delitos en particular*. Buenos Aires: Hammurabi.

Expediente 1123-D-2024. Proyecto de Ley. Código Penal de la Nación. Modificaciones sobre penas para el delito de extorsión y la difusión no consentida de material íntimo, de desnudez y/o de material que retrata violencia sexual. Cámara de Diputados de la Nación Argentina. https://www4.hcdn.gob.ar/dependencias/dsecretaria/Periodo2024/PDF2024/TP2024/1123-D-2024.pdf

Expediente 2757-D-2022. Proyecto de Ley. Código Penal de la Nación. Modificaciones penas para el delito de extorsión y la difusión no consentida de material íntimo, de desnudez y/o de material que retrata violencia sexual. Cámara de Diputados de la Nación Argentina. https://www4.hcdn.gob.ar/dependencias/dsecretaria/Periodo2022/PDF2022/TP2022/2757-D-2022.pdf

Expediente 2987-D-2019. Proyecto de Ley. Código Penal. Incorporación del artículo 155 bis, sobre penalización de la difusión no consentida de contenidos de desnudez total o parcial o contenido sexual. https://www2.hcdn.gob.ar/proyectos/textoCompleto.jsp?exp=2987-D-2019&tipo=LEY

FAITH CRANOR, L. (2010). Delincuencia informática. *Investigación y ciencia, 402* 70-75. https://dialnet.unirioja.es/servlet/articulo?codigo=3151630

FERNÁNDEZ DELPECH, H. (2014). *Manual de derecho informático.* Buenos Aires: AbeledoPerrot.

FERNÁNDEZ SANTIAGO, A. y CASTRO FUERTES, M. (2009). "Comentario al artículo 197 CP". En AMADEO GADEA, S. (Dir.). *Código Penal. Doctrina Jurisprudencial.*

Parte especial. Ed. Factum Libri Ediciones. http://0-vlex.com.cisne.sim.ucm.es/vid/comentario-articulo-codigo-penal-69108467

FERNÁNDEZ SANTIAGO, A. y CASTRO FUERTES, M.(2009). Comentario al artículo 197 CP. AMADEO GADEA, S. (Dir.). *Código Penal. Doctrina Jurisprudencial. Parte especial*. Ed. Factum Libri Ediciones. http://0-vlex.com.cisne.sim.ucm.es/vid/comentario-articulo-codigo-penal-69108467

FIGARI, R. E. (2009). *Reflexiones sobre la defraudación informática ley 26.388*. SAIJ. http://www.saij.gob.ar/ruben-enrique-figari-reflexiones-sobre-defraudacion-informatica-ley-26388-dacf100073-2009-08-12/123456789-0abc-defg3700-01fcanirtcod

FIGARI, R. E. (2018). Comentario al art. 128 del C.P. (Ley 27.436) sobre pornografía infantil. *Revista Derecho Penal y Criminología*, *7* (10) https://www.pensamientopenal.com.ar/index.php/system/files/2018/10/doctrina47068.pdf

FILLIA, L., MONTELEONE, R., NAGER, H., ROSENDE, E. y SUEIRO, C. Análisis a la reforma en materia de criminalidad informática al Código Penal de la Nación (Ley 26.388). *La Ley Revista Jurídica Argentina*, 938-964.

FOGGETTI, N. (2003). Análisis de un supuesto de delincuencia informática trasnacional. *Novática: Revista de la Asociación de Técnicos de Informática, 166*, 42-49.

FONTÁN BALESTRA, C. (2002). Derecho Penal. Parte Especial. Buenos Aires: LexisNexis Abeledo-Perrot.

FRAGA UTGES, V. (2022). La difusión no consentida de material íntimo, un análisis a la luz de la criminología feminista. *En V Jornadas de investigación en ciencia jurídica. Facultad de Derecho*, Buenos Aires, Argentina.

https://jornadasinvestigacion.der.unicen.edu.ar/wp-content/uploads/2022/09/Fraga-_-Calandra.pdf

FRANKS, M. A. (2016). Criminalizing Revenge Porn: Frequently Asked Questions. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2337998

GALÁN MUÑOZ, A. (2009). La internacionalización de la represión y la persecución de la criminalidad informática: un nuevo campo de batalla en la eterna guerra entre prevención y garantías penales. *Revista penal*, 24, 90-107. https://dialnet.unirioja.es/servlet/articulo?codigo=3129440&orden=0&info=link

GARRIDO MONTT, M. (2013). *Teoría del Delito. Derecho Penal. Parte General. Tomo II.* Chile: Editorial Jurídica.

GIANNANTONIO, E. (1987). *El valor jurídico del documento electrónico*. Buenos Aires: Editorial Depalma.

GONZÁLEZ HURTADO, (2013). *Delincuencia informática: daños informáticos del artículo 264 del Código Penal y propuesta de reforma*. Tesis doctoral. Universidad Complutense de Madrid. https://hdl.handle.net/20.500.14352/37980

GUTIÉRREZ FRANCÉS, M. L. (2005). Reflexiones sobre la ciberdelincuencia hoy. En torno a la ley penal en el espacio virtual. *Revista electrónica del departamento de derecho de la Universidad de La Rioja, 3*, 69-92. https://publicaciones.unirioja.es/ojs/index.php/redur/article/view/3858/3156

GUTIÉRREZ, R.; RADESCA, L, C. y RIQUERT, M. A. (2001). Violación de Secretos y de la Privacidad. *Revista Pensamiento Penal*. https://www.pensamientopenal.com.ar/system/files/cpcomentado/cpc37762.pdf

HERNÁNDEZ DÍAZ, L. (2009). El delito informático. *Eguzkilore, 23,* 227-243. https://www.ehu.eus/documents/1736829/2176697/18-Hernandez.indd.pdf

HUERTA MIRANDA, M. y LÍBANO MANZUR, C. (1996). *Los Delitos Informáticos*. Chile: Editorial Jurídica Cono Sur.

HUETE NOGUERAS, J. (2010). La reforma de los delitos informáticos. . *La Ley: Revista jurídica española de doctrina, jurisprudencia y bibliografía,, 7534*.

IBARRA, V. y NIEVES, M. (2016). La seguridad internacional determinada por un mundo on-line: el Estado ante el desafío del terrorismo y la ciberseguridad. En VIII Congreso de Relaciones Internacionales. http://ocs.congresos.unlp.edu.ar/index.php/CRRII/CRRII-VIII/paper/viewFile/3464/874

III Reunión del Grupo de Expertos Gubernamentales en materia de Delito Cibernético, 23 y 24 de junio, 2003. https://www.oas.org/juridico/spanish/recomenIII_sp.pdf

Informe de la Comisión al Consejo basado en el artículo 12 de la Decisión Marco del Consejo, 24 de febrero, 2005, relativa a los ataques contra los sistemas de información.

IX Reunión del Grupo de Expertos Gubernamentales en materia de Delito Cibernético, 12 y 13 de diciembre, 2016. http://www.oas.org/juridico/PDFs/ix_cyber_rec_MJ00773S01.pdf

IZQUIERDO LOYOLA, V. M. (1998). La administración pública y el mundo digital: desafíos para el futuro. *Revista iberoamericana de derecho informático, 27, 28 y 29.*

JAN DRIJBER, B. (1998). Enfoque común hacia el crimen organizado: el caso de la Unión Europea. En CARRASCOSA LÓPEZ, V. (Coord.). Jornadas Internacionales sobre el Delito Cibernético. *Informática y derecho. Revista iberoamericana de derecho informático*, (27- 29), 123-140. https://dialnet.unirioja.es/descarga/articulo/248141.pdf

JAN DRIJBER, B. (1998). Enfoque común hacia el crimen organizado: el caso de la Unión Europea. *Revista iberoamericana de derecho informático, 27, 28 y 29.*

LAMPERTI, S. (2014). *Problemáticas en torno a la investigación de los delitos informáticos Congreso Iberoamericano de Investigadores y Docentes de Derecho e Informática.*

CIIDDI. Sede: Mar del Plata. Universidad Fasta Federación Iberoamericana de Asociaciones de Derecho e Informática.

LARA, J. C.; MARTÍNEZ, M. Y VIOLLIER, P. (2014). Hacia una regulación de los delitos informáticos basada en la evidencia. *Revista Chilena de Derecho y Tecnología*, *3*(1), 101-137. https://rchdt.uchile.cl/index.php/RCHDT/article/view/32222/34151

LEINER, B.; CERF, V. y CLARK, D. (2003*). A brief history of Internet*. Washington: Internet Society.

Ley 11.723 (1933, 26 de septiembre). Régimen legal de la propiedad intelectual. Congreso de la Nación Argentina. Boletín Nacional. https://servicios.infoleg.gob.ar/infolegInternet/anexos/40000-44999/42755/texact.htm

Ley 11.723 de Propiedad Intelectual. (1933, 26 de septiembre). Congreso de la Nación Argentina. Boletín Nacional. https://www.argentina.gob.ar/normativa/nacional/ley-11723-42755/texto

Ley 25.326 (2000, 4 de octubre). Protección de los Datos Personales. Congreso de la Nación Argentina. Boletín Nacional. https://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm

Ley 26.388 (2008, 4 de junio). Código Penal. Modificación. Congreso de la Nación Argentina. Boletín Nacional. https://www.argentina.gob.ar/normativa/nacional/ley-26388-141790/texto

Ley 26.904 (2013, 13 de noviembre). Código Penal. Incorporación. Congreso de la Nación Argentina. Boletín Nacional. https://servicios.infoleg.gob.ar/infolegInternet/anexos/220000-224999/223586/norma.htm

Ley 27.411 (2017, 22 de noviembre). Convenio sobre Ciberdelito. Aprobación. Congreso de la Nación Argentina. Boletín Nacional. https://www.argentina.gob.ar/normativa/nacional/ley-27411-304798/texto

Ley 27.430 (2017, 27 de diciembre). Impuesto a las Ganancias. Modificación. Congreso de la Nación Argentina. Boletín Nacional. https://servicios.infoleg.gob.ar/infolegInternet/anexos/305000-309999/305262/norma.htm

Ley 27.436 (2018, 23 de abril). Código Penal. Modificación. Congreso de la Nación Argentina. Boletín Nacional. https://servicios.infoleg.gob.ar/infolegInternet/anexos/305000-309999/309201/norma.htm

Ley N° 19798 de Telecomunicaciones (1972, 23 de agosto). Congreso de la Nación Argentina. Boletín Nacional. https://www.argentina.gob.ar/normativa/nacional/ley-19798-31922/texto

Ley N° 25250 de Inteligencia Nacional (2001, 27 de noviembre). Congreso de la Nación Argentina. Boletín Nacional. https://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70496/norma.htm

Ley N° 25506 de Firma Digital (2001, 14 de noviembre). Congreso de la Nación Argentina. Boletín Nacional. https://www.argentina.gob.ar/normativa/nacional/ley-25506-70749

Ley N° 25930 de Modificación del Código Penal (2004, 21 de septiembre). Congreso de la Nación Argentina. Boletín Nacional. https://www.argentina.gob.ar/normativa/nacional/ley-25930-98807

Ley N° 27411 de Convenio sobre Ciberdelito. Aprobación (2017, 15 de diciembre). Congreso de la Nación Argentina. Boletín Nacional. https://www.argentina.gob.ar/normativa/nacional/ley-27411-304798/texto

Ley N° 27590 de Programa Nacional de Prevención y Concientización del Grooming o Ciberacoso contra Niñas, Niños y Adolescentes (2020, 16 de diciembre). Congreso de la Nación Argentina. Boletín Nacional. https://www.argentina.gob.ar/normativa/nacional/ley-27590-345231/texto

LEZERTUA RODRÍGUEZ, M. (2001). El Proyecto de Convenio sobre el cibercrimen del Consejo de Europa - proteger el ejercicio de derechos fundamentales en las redes informáticas. *Cuadernos europeos de Deusto, 25*, 83-117.

LEZERTUA RODRÍGUEZ, M. (2001). El Proyecto de Convenio sobre el cibercrimen del Consejo de Europa. Proteger el ejercicio de derechos fundamentales en las redes informáticas. *Cuadernos europeos de Deusto, 25*, 83-118. http://www.deusto-publicaciones.es/deusto/pdfs/revistas/revistas25.pdf

LÓPEZ ALONSO, M. (1998). La protección de los usuarios de Internet: auto regulación colegiada o leyes supranacionales. *Revista iberoamericana de derecho informático, 27, 28 y 29.*

LUCERO, P. Y KOHEN, A. (2011). *Delitos informáticos*. Buenos Aires: Ediciones D&D.

MAGRO SERVET, V. (2004). La delincuencia informática. ¿Quién Gobierna Internet? . *La Ley: Revista jurídica española de doctrina, jurisprudencia y bibliografía, 27* (6077).

MARTÍNEZ OTERO, J. M. (2014). El nuevo tipo delictivo del artículo 197.4 bis: la difusión no autorizada de imágenes íntimas obtenidas con consentimiento. *La Ley, 35* (8234). https://diariolaley.laleynext.es/Content/DocumentoRelacionado.aspx?params=H4sIAAAAAAAEAMtMSbF1CTEAAiMDU1NTI7Wy1KLizPw827DM9NS8klQArSdMYyAAAAA=WKE#nDT0000205552_NOTA6

MARTÍNEZ, M. (2018). *Algunas cuestiones sobre delitos informáticos en el ámbito financiero y económico. implicancias y consecuencias en materia penal y responsabilidad civil en Cibercrimen y delitos informáticos: los nuevos tipos penales*. En Parada, R. A. y

Errecaborde, J. D. (comp.). *La era de internet*. Ciudad Autónoma de Buenos Aires: Erreius.

MARTÍNEZ, M. S. (2009). *Hábeas data financiero.* Buenos Aires: Ediciones de la República.

MATARASSO, G. (2001, 28 de diciembre). Firma digital y firma electrónica (Ley 25.506). *Marval O'Farrell Mairal.* https://www.marval.com/publicacion/firma-digital-y-firma-electronica-ley-25506-4834?lang=es

Ministerio de Economía (2023). Ley Olimpia contra la violencia digital. https://portal.produccion.gob.ar/novedades/ley-olimpia-contra-la-violencia-digital--0166572842314-

Ministerio de Justicia (2021). Ciberdelito: Se aprobó el texto del 2° Protocolo Adicional del Convenio de Budapest. https://www.argentina.gob.ar/noticias/ciberdelito-se-aprobo-el-texto-del-2deg-protocolo-adicional-del-convenio-de-budapest

Ministerio de Justicia y Derechos Humanos (2021). *Ley de grooming en lectura fácil.* https://www.argentina.gob.ar/sites/default/files/2021/09/grooming-ley27590.pdf

Ministerio de Justicia y Derechos Humanos de la Nación (2015). *Manual de procedimiento para la preservación del lugar del hecho y la escena del crimen.* Programa Nacional de Criminalística. https://www.mpf.gob.ar/capacitacion/files/2015/07/Manual-Criminalistica.pdf

Ministerio de las Mujeres, Géneros y Diversidad (2022). Guía para la prevención de las violencias de género en entornos digitales. https://www.argentina.gob.ar/sites/default/files/2022/08/231030-guia_para_la_prevencion_de_las_violencias_de_genero_en_entornos_digitales-v7.pdf

MIRÓ LLINARES, F. (2010). *Delitos informáticos*: Hacking. Daños. En ORTIZ DE URBINA GIMENO, Í. (coord.). *Memento Experto. Reforma Penal*. Madrid: Ediciones Francis Lefebvre.

MOLINA, J. M. (1998). Criptología y delito informático. *Revista iberoamericana de derecho informático, 27, 28 y 29.*

MORABITO, M. R. (2010). La regulación de los "delitos informáticos" en el Código Penal Argentino. Nuevas tendencias criminológicas en el ámbito de los delitos contra la integridad sexual y la problemática de persecución penal. *La Ley – Thomson Reuters.* http://www.dab.com.ar/articles/10/la-regulaci%C3%B3n-de-losdelitos-inform%C3%A1ticos-en-el-c%C3%B3.aspx

MORAL TORRES, A. (1998). Colaboración policial internacional en el ciberespacio. En CARRASCOSA LÓPEZ, V. (Coord.). Jornadas Internacionales sobre el Delito Cibernético. *Informática y derecho. Revista iberoamericana de derecho informático*, (27- 29), 353-360. https://dialnet.unirioja.es/descarga/articulo/248184.pdf

MORAL TORRES, A. (1998). Colaboración policial internacional en el ciberespacio" en Informática y derecho. *Revista iberoamericana de derecho informático, 27, 28 y 29.*

MORALES GARCÍA, O. (2002). Apuntes de política criminal en el contexto tecnológico. Una aproximación a la convención del Consejo de Europa sobre Cyber-Crime. *Cuadernos de derecho judicial, 9,* 11-34.

MORILLAS CUEVA, L. y CRUZ BLANCA, M. J. (2009). "Informática y delito. Aspectos penales relacionados con las nuevas tecnologías." En BENÍTEZ ORTÚZAR, I. F. (Coord.). *Reformas del Código Penal. Respuestas para una sociedad del Siglo XXI*. Ed. Dykinson.

MORILLAS FERNÁNDEZ, D.L. (2005). *Análisis dogmático y criminológico de los delitos de pornografía infantil. Especial consideración de las modalidades comisivas relacionadas con Internet.* Dykinson.

MUÑOZ ESQUIVEL, O. (2002). La convención sobre delitos informáticos. AR: Revista de Derecho Informático, 42.

NOBLETT, M.; POLLITT, M. y PRESLEY, L. (2000): Recuperación y examen de evidencia en informática forense. *Revista Ciencias de la comunicación forense*, *4*(2).

Observatorio de la Ciberseguridad en América Latina y El Caribe (2016). *Ciberseguridad ¿Estamos preparados en América Latina y el Caribe? Informe Ciberseguridad.* https://www.oas.org/docs/cybersecurity/AgendaESP.mar2016.pdf

OCDE (1986). *Computer-related crime: analysis of legal policy. Information, computer and communications policy*. Washington: Ed. OECD Publications and Information Centre.

OCDE (1992). *Guidelines for the Security of Information Systems*. Washington: Ed. OECD Publications and Information Centre.

OCDE (2002). Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. Washington: Ed. OECD Publications and Information Centre. http://www.oecd.org/internet/interneteconomy/34912912.pdf

OEA (2003). *Declaración sobre seguridad de las Américas*. https://www.oas.org/36ag/espanol/doc_referencia/DeclaracionMexico_Seguridad.pdf

OEA (2016). Ciberdelito: 90.000 millones de razones para perseguirlo. https://www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=C-063/16

OEA (2021). *La violencia de género en línea contra las mujeres y niñas. Guía de conceptos básicos, herramientas de seguridad digital y estrategias de respuesta.* https://www.oas.org/es/sms/cicte/docs/Manual-La-violencia-de-genero-en-linea-contra-las-mujeres-y-ninas.pdf

OEA (s.f.). *Grupo de trabajo en Materia de Delito Cibernético.* https://www.oas.org/es/sla/dlc/cyber-es/grupo-trabajo.asp

OEA (s.f.). *Programas de Ciberseguridad.* https://www.oas.org/ext/es/seguridad/prog-ciber

ONU (1990). Informe general del 8º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal.

https://www.unodc.org/documents/congress/Previous_Congresses/8th_Congress_1990/028_ACONF.144.28.Rev.1_Report_Eighth_United_Nations_Congress_on_the_Prevention_of_Crime_and_the_Treatment_of_Offenders_S.pdf

ONU (1994). Manual de las Naciones Unidas sobre prevención y control de delitos informáticos. *Revista Internacional de Política Criminal*, 43.

ONU (1995). Informe general del 9º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal. https://www.unodc.org/documents/congress//Previous_Congresses/9th_Congress_1995/019_ACONF.169.16.REV.1_Report_of_the_9th_Crime_Congress_Overview_of_Agenda_S.pdf

ONU (2000). Informe general del 10º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal. https://www.unodc.org/documents/congress//Previous_Congresses/10th_Congress_2000/030_ACONF.187.15_Report_of_the_Tenth_United_Nations_Congress_on_the_Prevention_of_Crime_and_the_Treatment_of_Offenders_S.pdf

ONU (2005). Informe general del 11º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal. https://www.unodc.org/documents/congress/Documentation/11Congress/ACONF203_18_s_V0584412.pdf

ONU (2010). Informe general del 12º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal. https://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_18/V1053831s.pdf

OVILLA BUENO, R. (1998). Algunas reflexiones jurídicas en torno al fenómeno Internet. En CARRASCOSA LÓPEZ, V. (Coord.). Jornadas Internacionales sobre el Delito

Cibernético. *Informática y derecho. Revista iberoamericana de derecho informático,* (27- 29), 443-460. https://dialnet.unirioja.es/descarga/articulo/248210.pdf

OVILLA BUENO, R. (1998). Algunas reflexiones jurídicas en torno al fenómeno Internet" en Informática y derecho. *Revista iberoamericana de derecho informático, 27, 28 y 29.*

PALAZZI, P. (2000). *Derecho informático.* México: Mc Graw Hill.

PALAZZI, P. (2009). *Los Delitos Informáticos en el Código Penal, Análisis de la ley 26.388*. Buenos Aires: Abeledo Perrot.

PALAZZI, P. (2016). *Los Delitos Informáticos en el Código Penal. Análisis de la ley 26.388.* Buenos Aires: Abeledo Perrot.

PAVÓN PÉREZ, J. A. (2003). La labor del Consejo de Europa en la lucha contra la cibercriminalidad: El Protocolo Adicional al Convenio nº 185 sobre cibercriminalidad relativo a la incriminación de actos de naturaleza racista y xenófobos cometidos a través de los sistemas informáticos. *Anuario de la Facultad de Derecho de la Universidad de Extremadura, 21*. https://dehesa.unex.es/bitstream/10662/13231/1/0213-988X_21_187.pdf

PECOY, M. (2012). *Delitos informáticos*. Montevideo: Universidad de Montevideo.

PÉREZ GIL, J. (2004). Medidas de investigación y de aseguramiento de la prueba en el Convenio sobre el cibercrimen. *Actualidad penal, 36,* 895-933.

PIACENZA, D.F. (2009). Delitos informáticos. Revista de Derecho Informático, 127.

Portal Oficial del Estado (2023). Ley Olimpia: el Gobierno promulgó la legislación que incorpora la violencia digital como una modalidad de violencia de género. https://www.argentina.gob.ar/noticias/ley-olimpia-el-gobierno-promulgo-la-legislacion-que-incorpora-la-violencia-digital-como-una

Portal Oficial del Estado (2024). *¿Qué es la pornovenganza y cómo me protejo?* https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/que-es-y-como-protegerse-de-la-pornovenganza

Portal Oficial del Estado (s.f.). *Firma digital.* https://www.argentina.gob.ar/justicia/derechofacil/leysimple/firma-digital

Portal Oficial del Estado (s.f.). *Ley Mica Ortega - Prevención y concientización sobre grooming.* https://www.argentina.gob.ar/justicia/derechofacil/leysimple/ley-mica-ortega-prevencion-concientizacion-grooming

Portal oficial del Estado argentino (2024). ¿Qué es el phishing? https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/phishing

Portal oficial del Estado argentino (2024). Guía para padres y docentes: grooming. https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/guia-para-madres-padres-docentes-grooming#:~:text=Grooming%20es%20el%20acoso%20sexual,se%20llaman%20groomers%20o%20acosadores

Portal Oficial del Estado Argentino (s.f.). *Propiedad Intelectual.* https://www.argentina.gob.ar/justicia/derechofacil/leysimple/propiedad-intelectual

PRIETO ÁLVAREZ, V. y PAN CONCHEIRO, R. (2006). *Virus Informáticos.* Tesis para obtener el título de grado de Máster en Informática. Universidad Da Coruña. http://sabia.tic.udc.es/docencia/ssi/old/2006-2007/docs/trabajos/08%20-%20Virus%20Informaticos.pdf

Protocolo adicional al Convenio sobre la ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos. https://rm.coe.int/1680a7bbf3

QUINTERO OLIVARES, G. (2001). Internet y propiedad intelectual. En LÓPEZ ORTEGA, J. (Dir.) *Internet y derecho penal,10*, 367-398.

Resolución 1291/2019 (2019, 27 de noviembre). Unidad 24/7 de delitos informáticos y evidencia digital- Crease. Ministerio de justicia y derechos humanos. Boletín Nacional. https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-1291-2019-332246/texto

Resolución 144 / 2020 (2020, 31 de mayo). Protocolo general para la prevención policial del delito con uso de fuentes digitales abiertas. Ministerio de Seguridad. Boletín Nacional. https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-144-2020-338229/texto

Resolución 86 / 2022 (2022, 27 de diciembre). Programa de fortalecimiento en ciberseguridad y en investigación del cibercrimen (FORCIC). Ministerio de Seguridad. Boletín Nacional. https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-86-2022-360878/texto

Resolución AG/RES. 2004 (XXXIV-O/04). Adopción de una estrategia interamericana integral para combatir las amenazas a la seguridad cibernética: un enfoque multidimensionales y multidisciplinario para la creación de una cultura de seguridad cibernética, 8 de junio, 2004. https://www.oas.org/en/citel/infocitel/julio-04/ult-ciberseguridad_e.asp

RIBAS ALEJANDRO, J. (1998). La sociedad digital: riesgos y oportunidades. En CARRASCOSA LÓPEZ, V. (Coord.). Jornadas Internacionales sobre el Delito Cibernético. *Informática y derecho. Revista iberoamericana de derecho informático*, (27- 29), 51-62. https://dialnet.unirioja.es/descarga/articulo/248130.pdf

RIBAS ALEJANDRO, J. (1998). La sociedad digital: riesgos y oportunidades. Informática y derecho. *Revista iberoamericana de derecho informático, 27, 28 y 29.*

RIQUERT, M. (2016). Revelación de hechos, actuaciones, documentos y datos secretos. *Asociación Pensamiento Penal.* https://www.pensamientopenal.com.ar/system/files/art._157_revelacion_de_datos_secretos.pdf

RIQUERT, M. (2017). El "cibergrooming": nuevo art. 131 del C.P. y sus correcciones en el "Anteproyecto" argentino de 2014. *Asociación de Pensamiento Penal.* https://www.pensamientopenal.com.ar/system/files/2017/04/doctrina45151.pdf

RODRÍGUEZ BERNAL, A. (2007). España: Los Cibercrímenes en el Espacio de Libertad, Seguridad y Justicia. *AR: Revista de Derecho Informático, 103*.

RODRÍGUEZ BERNAL, A. (2007). España: Los Cibercrímenes en el Espacio de Libertad, Seguridad y Justicia. *AR: Revista de Derecho Informático, 103*.

RODRÍGUEZ BERNAL, A. (2007). España: Los Cibercrímenes en el Espacio de Libertad, Seguridad y Justicia. *Revista de Derecho Informático, 103.*

RODRÍGUEZ MOURULLO, G., LASCURAÍN SÁNCHEZ, J.A. y ALONSO GALLO, J. (2001). Derecho Penal e Internet. *Régimen jurídico de internet*, 257-310.

ROMEO CASABONA, C. M. (2006). Los datos de carácter personal como bienes jurídicos penalmente protegidos. *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas políticocriminales,* 167-190.

ROSENDE, E. (2008). Derecho penal e informática. Buenos Aires: Ed. Fabián Di Plácido.

ROVIRA DEL CANTO, E. (2002). *Delincuencia informática y fraudes informáticos.* Editorial Comares.

RUDI, J. (1994). *Las actas de 1984 y 1986 sobre delitos informáticos en los Estados Unidos de América.* E.D., T. 159 (1994-2)

SAEZ CAPEL, J. (2001). *Informática y delito*. Proa XXI.

SAIN G. y AZZOLIN H. (2017). *Delitos Informáticos*. Buenos Aires: B de F.

SAIN, G. (2012). *Delito y nuevas tecnologías: Fraude, narcotráfico y lavado de dinero por internet.* Buenos Aires: Editores del Puerto.

SAIN, G. (2013). *El Derecho Penal aplicado a los delitos informáticos: ¿Una política eficiente para el cibercrimen?* https://www.pensamientopenal.com.ar/system/files/2014/04/doctrina38470.pdf

SAIN, G. (2015). Evolución histórica de los delitos informáticos. *Revista Pensamiento Penal*.https://www.pensamientopenal.com.ar/system/files/2015/04/doctrina40877.pdf

SAIN, G. (2017). *Dificultades del proceso judicial en la investigación de delitos relacionados con dispositivos informáticos*. En AZZOLIN, H. y SAIN, G. *Delitos informáticos: investigación criminal, marco legal y peritaje*." Buenos Aires: BdeF.

SAIN, G. (2017). *Internet, el cibercrimen y la investigación criminal de delitos informáticos.* En AZZOLIN, H. y SAIN, G. *Delitos informáticos: investigación criminal, marco legal y peritaje*." Buenos Aires: BdeF.

SAIN, G. (2017). *La informática jurídica, el derecho informático y el cibercrimen*". Buenos Aires: Rubinzal-Culzoni

SAIN, G. (2018*). La estrategia gubernamental frente al cibercrimen: la importancia de las políticas preventivas más allá de la solución penal en Cibercrimen y delitos informáticos: los nuevos tipos penales*. En Parada, R. A. y Errecaborde, J. D. (comp.). *La era de internet*. Ciudad Autónoma de Buenos Aires: Erreius.

SAIN, G. R. (2012). Delito y nuevas tecnologías: fraude, narcotráfico y lavado de dinero por internet. Ciudad Autónoma de Buenos Aires: Editores del Puerto.

SALT, M. (1997). Informática y delito. *Revista Jurídica C.E.*

SÁNCHEZ BRAVO, A. A. (1998). La regulación de los contenidos ilícitos y nocivos en Internet: una propuesta desde la Unión Europea. En CARRASCOSA LÓPEZ, V. (Coord.). Jornadas Internacionales sobre el Delito Cibernético. *Informática y derecho.*

Revista iberoamericana de derecho informático, (27- 29), 361-388. https://dialnet.unirioja.es/descarga/articulo/248189.pdf

SÁNCHEZ BRAVO, A. A. (1998). La regulación de los contenidos ilícitos y nocivos en Internet" en Informática y derecho. *Revista iberoamericana de derecho informático, 27, 28 y 29.*

SÁNCHEZ BRAVO, A. A. (2002). El Convenio del Consejo de Europa sobre cibercrimen: control vs. libertades públicas. *La Ley: Revista jurídica española de doctrina, jurisprudencia y bibliografía, 3,* 1851-1859.

SÁNCHEZ MEDERO, G. (2009). *Internet: Un espacio para el cibercrimen y el ciberterrorismo.* Crisis analógica, futuro digital: actas del IV Congreso Online del Observatorio para la Cibersociedad. Ed. Meddia, cultura i comunicación.

SÁNCHEZ SISCART, J. M. (2011). Cibercrimen y cooperación judicial. Especial referencia a los ISP alojados en EE.UU. *Revista del poder judicial, 91,* 31-42.

SCHIFF BERMAN, P. (2005). From International Law to Law and Globalization. *Columbia Journal of Transnational Law, 43.*

SCHIFF BERMAN, Paul. (2005). From International Law to Law and Globalization. *Columbia Journal of Transnational Law, 43*(2).

SCHJOLBERG, S. (2008). *The history of global harmonization on cybercrime legislation. Road to Geneva.*

SCHULKIN, J. (2018, 13 de mayo). Argentina se suma a la Convención de Budapest para tratar delitos informáticos. *Infobae.* https://www.infobae.com/tecno/2018/05/13/argentina-se-suma-a-la-convencion-de-budapest-para-tratar-delitos-informaticos/

Segundo Protocolo adicional al Convenio sobre la Ciberdelincuencia, relativo a la cooperación reforzada y la divulgación de pruebas electrónicas. https://rm.coe.int/1680a83724

SIEBER, U. (1987). *The International Handbook on Computer Crime Computer-related Economic Crime and the Infringements of Privacy.* 1ª edición. Nueva Jersey: , Ed. John Wiley & Sons.

SIEBER, U. (1994). *Information Technology Crime. National Legislations and Internationals Initiatives.* Ed. Carl Heymanns Verlag.

SIEBER, U. (1998). *El problema: tipos comunes de delitos informáticos*. En Comisión Europea. *Aspectos legales de los delitos informáticos en la sociedad de la información.* Bruselas: Informe de la Comisión Europea.

SILVA SÁNCHEZ, J. M. (2002). La responsabilidad penal de las personas jurídicas en el Convenio del Consejo de Europa sobre cibercriminalidad. *Cuadernos de derecho judicial, 9,* 113-142.

SORBO. H. D. (2013). *Delitos Informáticos. Aspectos a tener en cuenta de la Ley 26.388.* https://server1.utsupra.com/doctrina1?ID=articulos_utsupra_02A00376672921

SOSA, M. E. (2024). Sextorsión: el problema de la falta de tipificación legal de esta práctica. *Revista Pensamiento Penal, 510.* https://www.pensamientopenal.com.ar/system/files/Sosa-sextorsi%C3%B3n.pdf

SWINBURNE, P. (1998). La cooperación internacional policial en el ciberespacio. Perspectiva UK. *Revista iberoamericana de derecho informático, 27, 28 y 29.*

TAZZA, A. (2014). El delito de grooming. *La Ley.*

TÉLLEZ VALDÉS, J. (1998). Delitos cibernéticos. En CARRASCOSA LÓPEZ, V. (Coord.). Jornadas Internacionales sobre el Delito Cibernético. *Informática y derecho. Revista iberoamericana de derecho informático,* (27- 29), 113-122. https://dialnet.unirioja.es/descarga/articulo/248139.pdf

TÉLLEZ VALDÉS, J. (1998). Delitos cibernéticos. Informática y derecho. *Revista iberoamericana de derecho informático, 27, 28 y 29.*

TÉLLEZ VALDÉS, J. (2003). Derecho informático. México: Ed. Mc Graw Hill.

TEMPERINI, M. (2014). *Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado.* 14º Simposio Argentino de Informática y Derecho, SID, 129-139. https://43jaiio.sadio.org.ar/proceedings/SID/13.pdf

TEMPERINI, M. (2016). Deep web, anonimato y cibercrimen. En VI Congreso Iberoamericano de Investigadores y docentes de derecho e informática.

TEMPERINI, M. (2018). *Delitos informáticos y cibercrimen: alcances, conceptos y características en Cibercrimen y delitos informáticos: los nuevos tipos penales*. En Parada, R. A. y Errecaborde, J. D. (comp.). *La era de internet*. Ciudad Autónoma de Buenos Aires: Erreius.

Universidad de Jaén (2018). Guía de Seguridad UJA. Correo electrónico no solicitado (SPAM). Servicio de Informática Vicerrectorado de Tecnologías de la Información y la Comunicación y Universidad Digital. https://www.ujaen.es/servicios/sinformatica/sites/servicio_sinformatica/files/uploads/guiaspracticas/Guias%20de%20seguridad%20UJA%20-%201.%20SPAM.pdf

UNODC (s.f.). *Mini guía de seguridad informática.* https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Safety_Guide_Spanish.pdf

V Reunión del Grupo de Expertos Gubernamentales en materia de Delito Cibernético, 19 y 20 de noviembre, 2007. http://www.oas.org/juridico/spanish/cyb_Vrec_sp.pdf

VANINETTI, H. A. (2013). Inclusión del grooming en el Código Penal. *La Ley.* https://es.scribd.com/document/430684085/27-Grooming-Vaninetti-pdf

VELASCO NÚÑEZ, E. (2006). "Cuestiones procesales relativas a la investigación de los delitos informáticos." En VELASCO NÚÑEZ, E. (Dir.). *Delitos contra y a través de*

las nuevas tecnologías. ¿Cómo reducir su impunidad? Ed. Consejo General del Poder Judicial, Cuadernos de Derecho Judicial.

VELASCO NÚÑEZ, E.: (2006). Aspectos procesales de la investigación y de la defensa en los delitos informáticos. *La Ley: Revista jurídica española de doctrina, jurisprudencia y bibliografía, 3*, 1857-1864.

VI Reunión del Grupo de Expertos Gubernamentales en materia de Delito Cibernético, 21 y 22 de enero, 2010. http://www.oas.org/juridico/english/cyb_VIrec_sp.pdf

VII Reunión del Grupo de Expertos Gubernamentales en materia de Delito Cibernético, 6 y 7 de febrero, 2012. http://www.oas.org/juridico/PDFs/VIIcyb_recom_sp.pdf

VIII Reunión del Grupo de Expertos Gubernamentales en materia de Delito Cibernético, 27 y 28 de febrero, 2014. http://www.oas.org/juridico/PDFs/VIIIcyb_recom_sp.pdf

VILLALBA DÍAZ, F. A. (2000). Los delitos y contravenciones informáticas: los hackers y el Código Contravencional de la Ciudad de Buenos Aires. *La Ley, Editor, 64*,(96).http://biblioteca.camdp.org.ar/docu/HACKERS.pdf

VIZCARDO, S. J. H. (2014). Tipificación de los delitos informáticos patrimoniales en la nueva ley de delitos informáticos N° 30096. *Derecho y Ciencia Política, 1*, 69-80. https://revistasinvestigacion.unmsm.edu.pe/index.php/alma/article/download/11870/10592/41319

VRIESDE, R. (1998). Investigaciones digitales. La perspectiva holandesa. *Revista iberoamericana de derecho informático, 27, 28 y 29.*

X Reunión del Grupo de Expertos Gubernamentales en materia de Delito Cibernético, 28 y 29 de abril, 2022. http://www.oas.org/es/sla/dlc/mesicic/docs/x_cyber_rec_final_esp.pdf

YAR, M. (2006). *Cybercrime and society*. London: Sage Publications.

ZARATE, P. y BECERRA, M. (2011). *Robo de identidad y su incidencia en el Cibercrimen.* En Simposio Argentino de Informática y Derecho. https://50jaiio.sadio.org.ar/pdfs/sid/SID-08.pdf

ZERDA, M. (2021). Violencia de Género Digital. Ciudad Autónoma de Buenos Aires: Hammurabi.