Columnas & Opinión

Revista Pensamiento Penal
Sección Medios digitales y delitos informáticos
Vol. 2, núm. 2 – 2025, págs. 116–125
ISSN: 1853 – 4554

Tras la huella digital del crimen

Un estudio sobre las organizaciones criminales digitales y sus actividades de ciberdelito

Por Lara Martina Barrios[1]

En un mundo donde las fronteras físicas se desvanecen y la tecnología conecta cada rincón del planeta, el crimen organizado ha encontrado nuevas y sofisticadas formas de operar, desde fraudes financieros hasta ataques a infraestructuras críticas y robos masivos de datos, lo que plantea serios desafíos para los Estados al poner en evidencia las limitaciones del sistema jurídico tradicional ¿Es posible que nuestra legislación evolucione lo suficientemente rápido para abordar los desafíos de la era digital, o quedaremos atrapados en un sistema legal obsoleto frente a la complejidad de los delitos cibernéticos?

*crimen organizado – ciberdelitos – delitos informáticos – ciberespacio – era digital – investigación judicial – prevención*

* * * * * *

a. Introducción

La nueva era digital en la que transitamos trae aparejada la aparición de nuevos paradigmas delictivos conocidos como *delitos informáticos*, los cuales vemos arraigarse a nuestra sociedad y que son utilizados no sólo por particulares, sino también cada vez más por organizaciones criminales como herramienta para llevar a cabo sus actividades ilícitas.

A través de un análisis exhaustivo, exploraremos la criminalidad organizada digital, partiendo del estudio del crimen organizado, y su rol dentro de este mundo digital.

El objetivo de esta investigación es proporcionar una visibilidad acerca del funcionamiento de las organizaciones, la manera en que trabajan para cometer estos delitos, las implicancias a la hora de probar los hechos, y finalizaré brevemente con algunas políticas, prácticas y medidas preventivas que promuevan un entorno digital más seguro para la sociedad.

b. Tecnología y delito

i. Ciberespacio

La constante evolución y el progreso tecnológico han dado lugar al denominado Quinto Dominio, el espacio cibernético. El término «ciberespacio» fue popularizado por la obra *Neuromancer*, una novela de

[1] Estudiante de Derecho en la Universidad de Buenos Aires (UBA). Correo electrónico: larabarrios621@gmail.com

ciencia ficción escrita por William Gibson publicada en 1984. Gibson entendía este mundo virtual como un

> «…espacio digital construido por muchos computadores en red, al que sólo podía accederse desde una terminal personal, mediante goggles y conexiones electrónicas entre el ordenador y el sistema nervioso, que permitía a los usuarios ingresar a una onírica mátriz que operaba como una alucinación consensual» (Giraldo, 2017, pág. 3).

Varios doctrinarios se han encargado de definir este espacio cibernético y es por ello que encontramos una gran variedad de conceptos y definiciones. No obstante, es necesario identificar algunos aspectos compartidos para entender mejor de qué se trata, y qué comprende.

Según lo describen los autores Claudio Paya-Santos y José María Luque-Juárez (2021), en principio se conforma de componentes tangibles o físicos. Ello es, por ejemplo, los dispositivos, las torres de telecomunicaciones, los cables, satélites y otros equipos que facilitan la conectividad digital global. Estos dispositivos a su vez incluyen nodos de acceso, que permiten a los usuarios acceder al ciberespacio, siempre y cuando tengan conexión a internet.

Por otro lado, los elementos intangibles, como la información, que se puede almacenar, transmitir o procesar por diferentes sistemas software. En el mundo digital encontramos desde servidores masivos que almacenan gran cantidad de datos, hasta una computadora personal. Por último, pero no menos significativo, el factor humano, esencial para la existencia del ciberespacio. Los seres humanos son responsables del mantenimiento y desarrollo de su infraestructura.

Para comprender su funcionamiento, debemos imaginar una red compleja que une a todo el mundo, no solo a través de Internet sino también mediante una infraestructura física y digital. El ciberespacio se extiende desde el espacio exterior hasta las profundidades marinas, permitiendo la transferencia de información en múltiples formas. Es interesante señalar que, a pesar de las numerosas ventajas que ofrece, actualmente algunos Estados deciden utilizarlo como herramienta en conflictos bélicos. Así fue lo que sucedió con el sabotaje de Israel a la capacidad nuclear de Irak, con el ataque informático perpetrado por un gusano virtual conocido como *Stuxnet*. Éste fue liberado en el año 2010, y atacó directamente las estaciones nucleares de Irán, dando *instrucciones de autodestruirse* (BBC NEWS Mundo, 2015), lo que nos lleva a plantear nuevos dilemas éticos y legales. ¿Es éste un uso indebido de la tecnología? ¿Cómo podemos garantizar la proporcionalidad y la discriminación en el uso de herramientas tecnológicas en conflictos armados? ¿Cuál es el papel de la comunidad internacional en la regulación y el control de estas acciones? A medida que la tecnología avanza, es crucial abordar estas cuestiones de manera integral y colaborativa para reducir los riesgos y garantizar la seguridad internacional.

ii. Delitos informáticos vs. delitos a través de medios informáticos

Para introducir el siguiente tema, utilizaré la definición de delitos informáticos que escribe el autor Gustavo A. Arocena en su artículo del año 2012, *la regulación de los delitos informáticos en el código penal argentino.*

El delito informático o ciberdelito es el injusto determinado en sus elementos por el tipo de la ley penal, conminado con pena y por el que el autor merece un reproche de culpabilidad, que, utilizando a los sistemas informáticos como medio comisivo o teniendo a aquéllos, en parte o en todo, como su objeto, se vinculan con el tratamiento automático de datos (Arocena, 2012).

Tal como expone el autor, el concepto de ciberdelito se compone de un elemento central imprescindible con el que se comete el delito, el sistema informático. Este actúa como el medio a través del cual se concreta la acción típica y antijurídica, para lo cual es esencial definir entonces, las nociones

básicas de lo que comprende un sistema informático. Para ello, nos remitiremos al Convenio de Budapest del año 2001, que en su artículo 1 define por sistema informático a «todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa» (Convenio de Budapest sobre ciberdelincuencia, 2001).

En otras palabras, estos sistemas contienen, en esencia, datos informáticos que actúan como instrucciones que se ejecutan de manera automática, permitiendo que operen de diversas formas. A continuación, ofreceré una breve explicación sobre su funcionamiento.

Toda esta información se transmite a través del espectro electromagnético, el cual emite una frecuencia electromagnética. Cuando esta frecuencia es muy alta, empieza a generar efectos materiales. Así es el caso de las ondas radioactivas o la energía nuclear, por ejemplo. Sin embargo, también existen otras frecuencias que pueden ser utilizadas para transportar datos. Ahora bien, ¿cómo se conectan estas redes? Aunque la mayoría podría pensar que los satélites son la principal herramienta de conexión, y esto no es incorrecto, ya que son una de las formas más comunes, en realidad existen múltiples métodos de conexión. Una quizás no tan conocida, es la comunicación por cables submarinos. Por ellos navega cualquier tipo de información que conozcamos, y son destinados fundamentalmente a servicios de telecomunicación. Sin embargo, es cuando se empieza a manipular esa información que comienzan a generarse los problemas, pues se compromete la privacidad y la seguridad de los datos transmitidos a través de estos cables, dando origen a lo que llamamos delitos cibernéticos.

El Convenio de Budapest sobre la Ciberdelincuencia, es el primer instrumento jurídico internacional que define y aborda específicamente los delitos informáticos, clasificándolos en dos categorías.

Los delitos propiamente cibernéticos, o también conocidos como ciberdependientes, son aquellos que necesariamente requieren de un medio informático para concretarse. Resulta interesante cuestionarnos si estos delitos existían, aunque de forma distinta, antes de la era digital, cuando no disponíamos de la infraestructura tecnológica ni la conectividad que nos proporcionan internet y los sistemas informáticos hoy en día. Parte de la doctrina argumenta que esta ciberdelincuencia introduce nuevos métodos y técnicas que requieren un enfoque legal diferente y la aplicación de normativas específicas.

Esta clase de delitos afecta tres pilares fundamentales de la seguridad de la información que se encuentra en las redes. Si bien no siempre afecta a los tres juntos, ya que podría ser solo uno o dos de ellos, genera desconfianza y puede derivar en una divulgación no autorizada de la misma.

En primer lugar, la confidencialidad, aquello que se debe resguardar. Hace referencia a la necesidad de ocultar determinada información o recursos. En segundo lugar, la integridad. Supone que la información se mantenga inalterada. Esta afectación puede producirse de manera total o parcial. Por último, la accesibilidad. Un claro ejemplo, se da al momento de querer ingresar a una página web, y que la misma se encuentre caída, es decir, sin funcionamiento para el particular. Se busca que un sistema informático se mantenga en buen funcionamiento sin experimentar accesos no autorizados. El Convenio sobre la ciberdelincuencia en el seno del Consejo de Europa, reconoce la necesidad de «prevenir los actos que pongan en peligro la confidencialidad, la integridad y la disponibilidad de los sistemas, redes y datos informáticos...» (Convenio de Budapest sobre ciberdelincuencia, 2001), investigando y sancionando dichas conductas delictivas.

Ahora bien, estas afectaciones desde el punto de vista legal permitirían no solo accionar penalmente, por las conductas antijurídicas reguladas en la Ley de Delitos Informáticos (Ley 26.388), sino también aplicándose, en casos de daños causados por acciones o negligencia en el uso de sistemas

informáticos, las normas sobre responsabilidad civil.

Como tiene dicho la doctrina: El daño informático se puede definir como toda lesión o menoscabo causado a un derecho subjetivo o interés legítimo mediante la utilización de medios electrónicos destinados al tratamiento automático de la información y que, concurriendo determinados presupuestos, genera responsabilidad (Leiva, 2005).

> «[...] El segundo plano recae en la gran diversidad de bienes jurídicos que pueden verse lesionados a través de Internet generando responsabilidad extracontractual, civil y penal, que es tan amplia como el Derecho mismo. Por lo tanto, la ilicitud es atípica y compartimos el criterio que sostiene que no cabe distinguir entre contenidos ilícitos y nocivos, ni entre antijuridicidad formal o material» (Brizzio, 2009).

Por otro lado, dentro de la categorización de delitos cibernéticos establecida por el Convenio de Budapest, existen otras conductas penadas que, aunque puedan involucrar el uso de tecnología avanzada, conservan un núcleo similar a los delitos tradicionales en cuanto a sus elementos legales y los efectos que generan en las víctimas.

Entre estos, destaca el caso del delito de estafa, consagrado en el artículo 172 del Código Penal de la Nación. Este delito ha existido durante siglos en diversas formas, pero la digitalización y el aumento en el uso de tarjetas de débito y crédito para operaciones comerciales, ha requerido de la adaptación de la normativa para abordar estos cambios, pues no se contemplaba primitivamente el fraude informático. En este contexto, los doctrinarios enseñan que

> «[…]en los casos de fraude informático es necesario descartar el error de la víctima llevada a cabo por el ardid o engaño del autor, pues este manipula una máquina con el objeto de obtener un beneficio económico en perjuicio patrimonial del afectado» (Parada & Errecaborde, 2018, pág. 41).

En consonancia con el avance tecnológico y mediante la reforma introducida por la Ley 25.930, se agregó al artículo 173 del Código Penal el inciso 15) que establece:

> «El que defraudare mediante el uso de una tarjeta de compra, crédito o débito, cuando la misma hubiere sido falsificada, adulterada, hurtada, robada, perdida u obtenida del legítimo emisor mediante ardid o engaño, o mediante el uso no autorizado de sus datos, aunque lo hiciere por medio de una operación automática».

Posteriormente, la ley de «Delitos Informáticos» (Ley 26.388) incorpora al mismo artículo, el inciso 16), el cual establece lo siguiente: «El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos».

De esta manera, las maniobras de fraude y estafa informática se asientan dentro del marco normativo, permitiendo su encuadre dentro de un tipo penal específico.

Parte de la doctrina sostiene que, en estos casos, es posible aplicar las leyes existentes sin necesidad de crear nuevas «categorías delictivas», en el sentido de que el delito propio preexistía a su consumación mediante sistemas informáticos. No obstante, en líneas generales, la adaptación de la legislación a la era digital es factible, sin perder de vista que nos enfrentamos a una criminalidad organizada compleja. Esta complejidad, derivada de las particularidades operativas y la dificultad probatoria de los delitos digitales, plantearía la necesidad de incorporar normativas específicas para abordarlas de manera adecuada.

c. Crimen organizado

i. Breve introducción

El denominado crimen organizado, constituye un concepto complejo y diversificado, dada la «ausencia de una conceptualización homogénea o consensual sobre el fenómeno» (Tokatlian, 1999, pág. 4). Esta falta de uniformidad, de una terminología precisa, generan confusión a la hora de entender conceptos como lo son el «crimen organizado» o las «redes criminales», generando en varias oportunidades, su tratamiento como categorías analíticas diversas.

Este fenómeno se presenta en la actualidad de manera recurrente, bajo distintas manifestaciones en formas extremadamente violentas, como lo son el tráfico de drogas o la trata de personas; o hasta en actividades aparentemente más sutiles, como el lavado de dinero o la corrupción. Este amplio abanico de actividades ilícitas demuestra la complejidad a la hora de definirlo.

Debemos destacar un aspecto fundamental respecto de la criminalidad organizada, siendo el criterio que la distingue: la «*organización*». La organización como parte de la estructura del delito, no es simplemente una entidad separada de las actividades ilícitas que se cometen, sino que se encuentra intrínsecamente ligada a la comisión de éstos. No solo es un medio, sino que forma parte especial de cómo se perpetran los mismos, pues conllevan una planificación, distribución de tareas y coordinación específica, «aumentando el grado de peligrosidad del mismo y repercutiendo, en última instancia, en el grado de reproche (culpabilidad) que se formule contra el autor del hecho» (Cordini, 2017, pág. 5).

La globalización y esta nueva era digital, ha transformado a este fenómeno, llevando a las organizaciones criminales a evolucionar de formas convencionales aprovechando la tecnología para mejorar u obtener una mayor facilidad en la realización de sus conductas delictivas. Esta transformación ha convertido a estas organizaciones en una seria amenaza para la sociedad en general, ya que ahora tienen la potencialidad de operar a escala global con relativa facilidad. Otro de los aspectos fundamentales a remarcar que caracterizan a estas organizaciones, es su finalidad económica. La ganancia financiera comprende una de las principales motivaciones detrás de sus actividades criminales, convirtiéndola en esencia, en una «empresa económica» (Clavería, 2011, pág. 6). Dada su naturaleza empresarial, la búsqueda constante de la maximización de los beneficios económicos, desemboca en la necesidad de una distribución del trabajo y una estructura jerárquica interna. Esta organización y digitalización de la *empresa*, permite reducir riesgos y aumentar la eficacia al introducir factores clave, como el anonimato, la coordinación remota para realizar transacciones ilícitas, el lavado de activos para su posterior integración al mercado legal y el uso de estos fondos para influir en sectores gubernamentales a través de actos de corrupción, permitiéndole así su permanencia.

Las organizaciones criminales digitales en particular han captado la atención de académicos, políticos, periodistas y expertos tanto a nivel nacional en Argentina, como a nivel internacional. Este enfoque destaca la importancia y el alcance de este fenómeno emergente en la discusión pública y la formulación de políticas, pues vemos día a día su crecimiento y la preocupación del Estado por controlarlas.

ii. Factor tecnológico en el crimen organizado

Producto de un mayor empleo por las organizaciones criminales de los sistemas informáticos para maximizar los beneficios de su estructura delictiva –falsificaciones, blanqueo de activos, comunicaciones anónimas, etc.- es que aumenta la capacidad de delinquir sin una efectiva persecución.

Es evidente que la finalidad o parte significativa del poder que tienen las organizaciones criminales ha cambiado su enfoque: si bien la constante búsqueda de riqueza, territorio o poder no ha desaparecido completamente, es posible que ahora se encuentre en menor medida.

En mi juicio, lo que pareciera ser realmente importante para una organización de este tipo hoy en día, es el control y la manipulación de información. Y qué mejor manera de lograrlo, que utilizando los sistemas informáticos y las redes comunicacionales que, como he mencionado anteriormente, almacenan una indeterminable cantidad de datos. Esto se debe a la profunda transformación del crimen organizado: ha migrado al ciberespacio.

Así fue como lo mencionó la Organización de las Naciones Unidas, en su Octavo Congreso sobre la Prevención del Delito y Tratamiento del Delincuente, señalando el uso que podían darle las organizaciones criminales al internet y las nuevas tecnologías. En ese marco, advirtió que «la delincuencia organizada puede utilizar dichas técnicas para fines tales como el blanqueo de dinero o para la gestión y transferencia de activos adquiridos ilegalmente» (ONU, 1991).

El criminalista Lic. Eduardo Muñoz (2024) expone una serie de factores, que enunciare a continuación, los cuales nos ayudan a entender esta transformación:

a. Anonimato: facilita operar de manera anónima, escondiendo la identidad y utilizando, redes privadas virtuales (VPN) o software de cifrado, lo que dificulta su rastreo por las autoridades.
b. Alcance internacional: permite llegar a víctimas en todo el mundo sin restricciones geográficas.
c. Lavado de dinero y monedas virtuales: las criptomonedas, son transacciones difíciles de rastrear, se utilizan como herramienta ideal para configurar el delito de lavado de dinero. Al ser un fenómeno relativamente nuevo, y la poca regulación que conlleva, permite blanquear activos deslizándose de sus orígenes ilícitos.
d. Menor riesgo físico: sin la necesidad de encuentros presenciales, se minimiza el riesgo de enfrentamientos con las fuerzas de seguridad.
e. Coordinación remota: la tecnología permite coordinar las actividades delictivas desde cualquier lugar con acceso a Internet.

Es decir, la tecnología ha transformado la forma en que operan las organizaciones criminales, brindándoles nuevas oportunidades para cometer delitos, así como también desafíos para las autoridades encargadas de su persecución.

iii. Problemática probatoria de las investigaciones

Clara es la ventaja que tienen las organizaciones criminales digitales para delinquir mediante sistemas informáticos. Del mismo modo, podríamos inferir que las autoridades estatales tienen ventajas al llevar a cabo investigaciones criminales en este ámbito. Sin embargo, es fundamental reconocer que surgen una serie de dificultades que obstaculizan la continuación del proceso legal y la captura de los sospechosos.

En primer lugar, dada la naturaleza trasnacional de las organizaciones criminales, una de las problemáticas más frecuentes es el fracaso o caída de las investigaciones internacionales, como así también las peticiones de extradición. Varios intentos fallidos de cooperación internacional pusieron en la atención del Consejo de Europa, la problemática sobre la falta de acuerdo de los Estados en cuestiones básicas en miras a «prevenir la criminalidad en el ciberespacio» (Lamperti, 2014, pág. 3), concluyendo en la creación del Convenio de Ciberdelincuencia, ratificado por Argentina en el año 2008. Entre sus principales logros, se precisaron cuestiones terminológicas y se clasificaron los delitos informáticos dentro de sus disposiciones.

Sin embargo, expone Sansó Rubert que:

> «Cada vez con mayor frecuencia, los operativos policiales son desarrollados por equipos multinacionales de forma simultánea en varios países, a pesar de las inherentes dificultades de organización y coordinación que conllevan, pero su coste se ve

> sobradamente recompensado por sus elevados índices de eficacia» (2005, pág. 13).

Por ejemplo, la INTERPOL (Organización Internacional de Policía Criminal) cuenta con cinco grupos de trabajos regionales sobre ciberdelincuencia en África, las Américas, Asia, Europa y Próximo Oriente, en los cuales se reúnen periódicamente para formular políticas y proyectos para combatir la ciberdelincuencia.

En segundo lugar, la dificultad de identificar o demostrar la participación de una, o varias personas, dado el anonimato del sujeto activo, ya que este se puede valer de un tercero, o del uso de programas de enmascaramiento que no permiten ver la verdadera dirección, ya sea de correo electrónico o del número IP (protocolo de internet que nos permite conectarnos, y la manera en que nuestra prestadora de servicios nos identifica).

Además, otro de los frecuentes problemas que se presentan corresponde a la determinación de la jurisdicción para su investigación. Dice la Resolución PGN N° 33/23 del Ministerio Público Fiscal en materia de criptomonedas

> «[...] Por último, otro factor relevante que dificulta la investigación penal en torno a los criptoactivos es la ubicación geográfica de sus operaciones y actores intermediarios, dado que estas ocurren en internet, desde todo tipo de dispositivos y en cualquier parte del mundo. Esto puede generar problemas para establecer cuál es el país donde se realizó la actividad delictiva y, con ello, la determinación de la jurisdicción para su investigación y juzgamiento [...]».

Así menciona la Dra. Lamperti (2014), que una de las soluciones propuestas en la doctrina, era la de aplicar una solución similar a los delitos de piratería, que se traduce en la «otorgación de competencia al país en cuyo poder caigan los delincuentes» (Lamperti, 2014, pág. 10).

Por último, si bien podrían mencionarse muchos otros factores que inciden en las investigaciones, resulta pertinente concluir con la complejidad técnica de la propia prueba. En las investigaciones y recolección de pruebas digitales, es esencial contar con conocimientos especializados en tecnología de la información y seguridad informática. Por ello, los «equipos forenses digitales» deben tener la capacidad de comprender esta complejidad técnica para garantizar una recopilación adecuada y eficiente de las pruebas. En este sentido, la INTERPOL promueve instancias de cooperación y actualización técnica mediante encuentros internacionales, tales como la Reunión del Grupo de INTERPOL de Expertos en Análisis Forense Digital, la Reunión del Grupo de INTERPOL de Expertos en Ciberamenazas contra la Automoción y en Investigación Forense de Vehículos, y el Foro de INTERPOL de ciencias forenses digitales aplicadas a los aparatos náuticos, donde se analizan casos, se discuten desafíos emergentes y se difunde información sobre los avances tecnológicos en la materia.

d. Políticas de prevención

A nivel internacional, varias instituciones intergubernamentales llevan adelante mecanismos de coordinación para denunciar e investigar presuntas actividades delictivas que son facilitadas por el uso de sistemas informáticos, así como la EUROPOL, la INTERPOL, o la BSI.

La EUROPOL (Agencia de la Unión Europea para la Cooperación Policial) es el centro de operaciones para la cooperación policial en Europa. Ayuda a los países miembros a trabajar juntos contra la delincuencia organizada, el terrorismo y la ciberdelincuencia, compartiendo información y coordinando acciones para las investigaciones que se llevan a cabo a la par con varios Estados (European Union Agency for Law Enforcement Cooperation, 2025).

La INTERPOL (Organización International de Policía Criminal) es una organización intergubernamental que cuenta con 196 países miembros. En cada

país, una Oficina Central Nacional (OCN) de INTERPOL actúa como punto de contacto para la Secretaría General, quien coordina las actividades para combatir distintos delitos.

Esta organización, International Criminal Police Organization, cuenta con siete objetivos policiales mundiales, que fueron respaldados por los países miembros de ella, con el fin de abordar una amplia gama de problemas relacionados con la delincuencia y la seguridad.

La BSI (Oficina Federal para la Seguridad en la Tecnología de la Información) es la autoridad nacional de Alemania de ciberseguridad que garantiza la seguridad de la información para el Estado y la sociedad. Entre sus principales tareas se encuentra la divulgación de información sobre seguridad informática y seguridad en internet, el desarrollo de sistemas de cifrado, la prueba y certificación de servicios informáticos, entre otros.

Además, Argentina en el año 2023 se adhirió al Segundo Protocolo Adicional del Convenio de Budapest de la Unión Europea, el cual es un adicional del Convenio de Budapest, principal herramienta de cooperación internacional en materia de ciberdelito, para agilizar las investigaciones en la materia (Argentina.gob.ar, 2023).

A nivel local, como respuesta a las constantes amenazas y delitos vinculados al crimen organizado, particularmente los cometidos por la banda narcotraficante operante en Rosario, el Ministerio de Justicia ha anunciado una serie de medidas orientadas a resolver la problemática delictiva. Entre ellas se incluyen: la implementación del sistema acusatorio con foco en el narcotráfico; el inicio de un proceso de reforma del Código Penal para incorporar nuevas figuras delictivas y aumentar las penas existentes para el narcotráfico, el crimen organizado y delitos asociados; el impulso de mecanismos para acelerar los procesos de decomiso y remate de los bienes provenientes del narcotráfico, y el fortalecimiento de la delegación local de la UIF (Unidad de Información Financiera), creada en el año 2023 mediante la Res. 31/2023(Comunicado de prensa del 13 de marzo, 2024).

En el año 2022 además, mediante la Resolución 86/22 del Ministerio de Seguridad, se crea el Programa de Fortalecimiento en Ciberseguridad y en Investigación del Cibercrimen (ForCIC) que tiene como objetivo principal coordinar, asistir y brindar asesoramiento en técnicas de seguridad de las infraestructuras digitales.

Menciona en la misma las recomendaciones que ha hecho la Organización de las Naciones Unidas, a través del informe de la Reunión de Grupos de Expertos, sobre las acciones y recursos que deberían integrar los Estados para combatir el delito cibernético.

Otra importante Resolución es la N° 1107-E/2017 la cual crea el Comité de Respuesta de Incidentes de Seguridad Informática del Ministerio de Seguridad (CSIRT), «cuyo objetivo principal es la coordinación de las actuaciones centralizadas ante usos nocivos y/o ilícitos de las infraestructuras tecnológicas, las redes y los sistemas de información y de telecomunicaciones del Ministerio y sus órganos dependientes» (RESOL-2022-86-APN-MSG, 2022).

Finalmente, por medio de la Acordada N° 32/2023, la Corte Suprema de Justicia de la Nación dispuso la creación de la Oficina de Ciberseguridad que tendrá como misión gestionar la seguridad del tribunal en materia de ciberdelincuencia, garantizando «la integridad, confidencialidad y disponibilidad de la información y sistemas, mediante una gestión proactiva frente a amenazas cibernéticas y promoviendo una cultura robusta de seguridad informática» (Acordada N° 32/2023, 2023).

e. Conclusiones

En síntesis, las organizaciones criminales digitales representan una forma moderna y sofisticada de criminalidad que aprovecha las nuevas tecnologías, para llevar a cabo una amplia gama de actividades delictivas.

Hemos analizado a lo largo de esta investigación, las constantes operaciones de

delincuencia organizada, el uso de sistemas informáticos como medio imprescindible de su desarrollo y la obtención de beneficios tanto económicos como procedimentales.

También hemos analizado los desafíos que enfrentan las autoridades en la lucha contra estas redes criminales, incluida la dificultad para obtener pruebas sólidas, el anonimato de los integrantes, la falta de cooperación internacional primitiva y la necesidad de adoptar legislaciones específicas, que se encuentren a la par de la complejidad que conllevan estas organizaciones.

La propensión a la cooperación global no es una ilusión, de hecho, cada vez más Estados reconocen la necesidad de tomar medidas en esta materia, y formar parte del Convenio sobre Ciberdelincuencia.

Es fundamental adoptar enfoques innovadores y estrategias integrales que aborden tanto las dimensiones tecnológicas como sociales de este fenómeno, con el objetivo de proteger la seguridad y permanencia de los ciudadanos en el ciberespacio.

En este sentido, les propongo una serie de recomendaciones orientadas a la prevención del delito informático y al fortalecimiento de la seguridad a la hora de navegar por internet:

a. Especial atención con los correos electrónicos SPAM o aquellos que contienen archivos adjuntos que desconocemos.

b. Actualizar los softwares de tus dispositivos cuando se encuentre disponible la misma, ya que corrigen vulnerabilidades de seguridad.

c. Revisar los permisos de las aplicaciones antes de instalarlas.

d. Revisar detenidamente los mensajes que nos llegan al teléfono celular, pues muchas veces logran parecer seguros y auténticos, pero en verdad es uno de los medios más utilizados en la actualidad para ingresar a las billeteras virtuales.

e. Comprobar que la dirección de la página cuente con el prefijo «https» y tenga un candado verde cerrado.

f. Bibliografía

Argentina.gob.ar. (2023). Obtenido de https://www.argentina.gob.ar/noticias/argentina-y-la-union-europea-unen-esfuerzos-para-combatir-el-ciberdelito

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.*, 945-988. Obtenido de http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0041-86332012000300002&lng=es&tlng=es

BBC NEWS Mundo. (2015). Obtenido de https://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet

Brizzio, C. R. (2009). *Sistema Argentino de Información Jurídica - SAIJ*.

Clavería, J. R. (2011). El crimen organizado. Guatemala. Obtenido de https://www.galileo.edu/pdh/wp-content/blogs.dir/17/files/2011/04/EL_CRIMEN_ORGANIZADO-IES.pdf

Cordini, N. S. (2017). El «crimen organizado»: un concepto extraño al derecho penal argentino. *SciELO Brasil*, 22. Obtenido de https://doi.org/10.1590/2317-6172201713

Europa, C. d. (23 de Noviembre de 2001). Convenio de Budapest sobre ciberdelincuencia.

EUROPOL. (2025). *European Union Agency for Law Enforcement Cooperation*. Obtenido de https://www.europol.europa.eu/about-europol:es

Giraldo, A. A. (2017). El ciberespacio y el problema de la realidad virtual. *Revista Filosofía UIS, 16*(2), 1-5. Obtenido de http://portal.amelica.org/ameli/jatsRepo/408/4081880010/index.html

INTERPOL. (2025). *International Criminal Police Organization*. Obtenido de https://www.interpol.int/es

Justicia., M. d. (2024). Comunicado de prensa del 13 de marzo. Obtenido de https://www.argentina.gob.ar/noticias/el-ministerio-de-justicia-presento-sus-acciones-contra-el-narcotrafico-0

Lamperti, S. (2014). Problemáticas en torno a la investigación de los delitos informáticos. Obtenido de http://redi.ufasta.edu.ar:8082/jspui/handle/123456789/1561

Leiva, C. F. (2005). *Sistema Argentino de Información Jurídica - SAIJ*. Obtenido de http://www.saij.gob.ar/claudio-fabricio-leiva-responsabilidad-danos-derivados-internet-reparacion-prevencion-danos-dacc050074-2005/123456789-0abc-defg4700-50ccanirtcod

Muñoz., E. (2024). «Crimen organizado en la era digital: adaptación y desafíos». *MDZ*. Obtenido de https://www.mdzol.com/sociedad/2024/4/24/crimen-organizado-en-la-era-digital-adaptacion-desafios-422492.html

Nación., C. S. (02 de 11 de 2023). Obtenido de https://www.csjn.gov.ar/documentos/descargar?ID=140180

ONU. (1991). Octavo Congreso de las Naciones Unidas sobre prevención del delito y tratamiento del delincuente. 149. Nueva York. Obtenido de 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

Parada, R. A., & Errecaborde, J. D. (2018). En *Cibercrimen y Delitos Informáticos: Los nuevos tipos penales en la era de internet*. (pág. 192). Ciudad Autónoma de Buenos Aires: Erreius.

Sansó-Rubert, D. (2005). La internacionalización de la delincuencia. *UNISCI Discussion Papers*, 1-19.

Seguridad, M. d. (11 de 02 de 2022). *Sistema argentino de información jurídica - SAIJ*. Obtenido de http://www.saij.gob.ar/encuestas/GetInfoleg?id=360878

Tokatlian, J. G. (1999). *Anotaciones en torno al crimen organizado, la seguridad nacional y la política internacional en relación al tema de las drogas psicoactivas: una aproximación conceptual a partir de la experiencia de Colombia*. Obtenido de https://home.udesa.edu.ar/files/humanidades/DT%2017%20-%20Juan%20G.pdf