Artículos

Revista Pensamiento Penal
Sección medios digitales y delitos informáticos
Vol. 1, núm. 3 – 2025, págs. 27–39
ISSN: 1853 – 4554
DOI: https://doi.org/10.64178/ 647bb124

Hacia una noción conceptual de los delitos informáticos en el Derecho penal argentino

Juan Ignacio Diaz[1]

Resumen

En este trabajo se analizarán las distintas definiciones y clasificaciones de los delitos informáticos, con el fin de proponer una noción conceptual uniforme en el derecho penal argentino. Se relevará la normativa nacional e internacional vigente, dado que el Código Penal argentino no contempla una definición ni un título específico sobre esta materia. El objetivo es establecer una definición clara y operativa que oriente la competencia y la investigación penal especializada. En definitiva, se busca arribar a una conclusión crítica y fundamentada sobre la conceptualización de los delitos informáticos en el ámbito de la criminalidad cibernética.

Sumario

Palabras clave

Código Penal de la Nación – delitos complejos – delitos informáticos – criminalidad cibernética – reforma legislativa

[1] Abogado, especialista en derecho penal, especialista en docencia universitaria; profesor adjunto de derecho penal especial, Facultad de Ciencias Jurídicas y Políticas, Instituto de Investigaciones Científicas (IDIC), Universidad de la Cuenca del Plata, Corrientes, Argentina. Correo electrónico: juanignaciodiazok@gmail.com
El presente trabajo surge en el marco del Proyecto de Investigación: «*Un Análisis Constitucional de los Delitos Informáticos en el Código Penal Argentino*» (UCP, Resolución N° 920/23, Fecha: 23/11/2023), Facultad de Ciencias Jurídicas y Políticas, Instituto de Investigaciones Científicas (IDIC), Universidad de la Cuenca del Plata, Corrientes, Argentina. Agradezco especialmente la colaboración y la destacada contribución a la Dra. Adriana Belén Pujol en el desarrollo del presente trabajo.

1. Introducción

En el presente trabajo se abordarán las distintas definiciones y clasificaciones de los delitos informáticos[2] a fin de llegar a una noción conceptual uniforme en el derecho penal argentino. En ese marco se efectuará un relevamiento de la normativa nacional e internacional referente a la temática de los delitos informáticos. Este estado de cosas a indagar resulta importante debido a que el Código Penal argentino no brinda una definición de delitos informáticos, ni tampoco existe en dicho cuerpo normativo un título dedicado exclusivamente sobre este tema.

La finalidad de este trabajo no es solamente teórica, sino también práctica. Se busca alcanzar una noción conceptual de los delitos informáticos en el Código Penal argentino, delimitando su alcance y contenido indispensable para orientar y determinar la competencia necesaria para llevar a cabo una correcta investigación penal especializada.

Al mismo tiempo, resulta importante diferenciar cuando estamos frente a un delito ordinario (homicidio, lesiones, abuso sexual, robo, etc.) y un delito informático. Determinar la existencia de un delito informático y su tipo permite entre otras cuestiones: a) que la recolección de evidencia digital esté confiada a organismos especializados en la temática (fiscalías especializadas en ciberdelitos[3]; fuerzas de seguridad y policiales[4], etc.); b) utilizar herramientas exclusivas para garantizar una adecuada seguridad informática; c) asegurar la intimidad personal, privacidad y datos de la presunta víctima.

Por otro lado, la informática es un tema cada vez más importante en la sociedad actual, ya que el aumento de la tecnología y su impacto en las vidas de las personas resulta sustancial, y casi imprescindible. Hoy, por ejemplo, los relevamientos nos muestran que existen más celulares -en funcionamiento- que personas en Argentina[5]. El celular con acceso a internet y las diferentes aplicaciones (apps) se han convertido en un brazo más del individuo para vivir.

En el mundo de la informática se encuentran todas las posibilidades, ya sea para realizar trabajos remotos (home office) y también para lesionar o dañar a personas, inclusive para lucrar de forma ilícita. En este submundo, llamado «*ciberespacio*», surgen los «*ciberdelincuentes*» que con el correr de los años fueron desarrollando sus habilidades técnicas para cometer distintas clases de delitos. Un dato, el derecho penal en este campo viene corriendo de atrás, es decir que existen varias conductas no tipificadas en el Código Penal, o bien que datan de una reciente sanción positiva.

En efecto, se ha señalado que la delincuencia informática tiene varios años de gestación, desarrollo y práctica. Dichas prácticas están destinadas generalmente a lucrar de forma no convencional, es decir, de una forma no legal (ilícita). En conclusión, los

---

[2] Indistintamente, se emplearán como sinónimos de «*delitos informáticos*» las expresiones: «*ciberdelitos*», «*delitos cibernéticos*», «*delitos electrónicos*», «*delitos telemáticos*», «*delitos computacionales*» y «*delitos del ciberespacio*».

[3] En Argentina, mediante la Resolución PGN N.º 3743/15, el Ministerio Público Fiscal de la Nación creó la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI), organismo encargado de la prevención, detección e investigación de delitos informáticos. Recuperado el 01/05/2024 de: https://www.mpf.gob.ar/ufeci/

[4] A través de la Resolución N.º 234/2016, el Ministerio de Seguridad aprobó el *Protocolo General de Actuación para las Fuerzas Policiales y de Seguridad en la Investigación y Proceso de Recolección de Pruebas en Ciberdelitos*. Recuperado el 02/05/2024 de: https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-234-2016-262787

[5] Según un informe periodístico, «Argentina tiene 59 millones de celulares activos: 9 de cada 10 son prepagos» (*Cadena 3*, 01/06/2024). Recuperado de: https://www.cadena3.com/noticia/tecnologia/argentina-tiene-59-millones-de-celulares-activos-9-de-cada-10-son-prepagos_356551

delitos informáticos ya son parte del fenómeno criminal, no obstante, no deja de sorprender cómo viene creciendo la ciberdelincuencia (Temperini, 2018).

Retomando, la dogmática penal se ha encontrado con un novedoso desafío que es definir y clasificar las modalidades delictivas que se dan en el círculo de las Tecnologías de la Información y la Comunicación (TIC). En este sentido, las llamadas TIC se han definido como el conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones (app), redes y medios que admiten la compilación, procesamiento, almacenamiento y transmisión de información, como, por ejemplo: voz, datos, texto, video e imágenes, etc.[6].

En términos generales, se entiende con razón que el delito informático es aquella acción ilícita que se realiza usando los medios de las Tecnologías de la Información y la Comunicación (TIC). Estos delitos pueden ser variados y comprenden desde el robo de datos personales hasta la violación de la intimidad, traspasando por el daño informáticos de un sistema de datos, así como también el acceso no autorizado a sistemas informáticos. En este contexto, se debe expresar que no existe uniformidad en la definición de delitos informáticos, ni tampoco en su clasificación como tal.

Con la finalidad de diferenciar la criminalidad cibernética en el ámbito del derecho penal, se establecerá una definición y clasificación de los delitos informáticos, basándose en las responsabilidades que Argentina ha adquirido para prevenir, investigar, reprimir y erradicar este tipo de delitos. En definitiva, el propósito es arribar a una conclusión razonada y crítica sobre la conceptualización de los llamados «delitos informáticos» en el derecho penal argentino

2. La normativa nacional e internacional referente a los delitos informáticos

En Argentina, el Código Penal de la Nación fue sancionado en el año 1921 y entró en vigencia en 1922, con el devenir de los años el cuerpo normativo mencionado ha sufrido innumerables modificaciones. Estas reformas del Código Penal obedecieron a diferentes motivos, entre ellas, obligaciones internacionales que el Estado argentino se ha comprometido a cumplir.

Así, el Convenio sobre Cibercriminalidad registrado en Budapest el 23 de noviembre del año 2001, fue incorporado al ordenamiento jurídico argentino a través de la Ley N° 27.411, y publicado en el Boletín Oficial el 15 de diciembre del año 2017.

Al respecto, ha explicado Flores Cáceres (2023) que el «Convenio de Budapest» se localiza por ser el primer instrumento legal de carácter internacional relacionado a los delitos informáticos. Dicho tratado internacional aborda la ciberdelincuencia, así como también los ciberdelitos determinando medidas de prevención, investigación y sanción.

En este contexto, emergen los denominados delitos informáticos en el ámbito del derecho penal argentino. A diferencia de los delitos tradicionales, que suelen desarrollarse en territorios donde las circunstancias son fácilmente identificables, los delitos telemáticos ocurren en el ciberespacio, un entorno caracterizado por la interconexión de redes que lo hacen universal. Esta naturaleza virtual de los ciberdelitos presenta un

[6] Ente Nacional de Comunicaciones (ENACOM). (s.f.). *¿Qué son las TIC y para qué sirven?* Recuperado el 10/05/2024 de: https://www.enacom.gob.ar/tic/que-son-las-tic-y-para-que-sirven_n1887

desafío significativo, ya que dificulta la identificación y determinación de los hechos ilícitos.

John Lennon, en la canción «*Imagine*», relató que imaginemos un mundo donde no haya países, donde el mundo sea uno, (…) imagina toda la gente compartiendo todo el mundo[7]. Bueno, con el internet se ha creado un mundo espacial, un ciberespacio, rompiendo las fronteras y límites entre las personas, es eso, el mundo compartiendo todo, desde su vida, libertad, intimidad, privacidad, información, comunicación, trabajo, operaciones económicas, negocios, etc., de forma inmediata y sin barreras entre los individuos que interactúan entre sí. Inclusive, con los móviles celulares y los bajos costos para acceder a internet permiten de forma accesible la comunicación y relación entre los individuos (ej.: Facebook, Instagram, WhatsApp, YouTube, etc.), así como también cualquier actividad cotidiana (ej.: registros documentales, transferencias bancarias, firma de contratos, compraventa bienes y servicios, etc.).

Las ventajas son muy evidentes, ya que permiten una globalización significativa en el ámbito de las comunicaciones y la información en la sociedad. Pero, las desventajas también son palmarias debido a que resulta más fácil lesionar bienes jurídicos, sin riesgo casi para el criminal. En este contexto, el Convenio de Budapest propone una política criminal internacional, integral y ordinaria para todos los Estados, direccionada a prevenir conductas ilícitas que afecten los sistemas de información, redes, datos informáticos, integridad y confidencialidad, así como también el abuso de la informática, redes y datos para ejecutar otros delitos.

3. Los diferentes conceptualizaciones y clasificaciones de los delitos informáticos

Como punto de partida para comenzar a discutir sobre la noción de delitos informáticos, se debe explicar que la informática será el elemento central para la configuración del delito. Para el Diccionario de la Real Academia Española el vocablo informático es el «*conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores*»[8].

Por otra parte, la expresión «sistema informático» debe ser entendida como «todo dispositivo o grupo de elementos relacionados que realiza el tratamiento automatizado de datos, generando, enviando, recibiendo, procesando o almacenando información de cualquier forma y por cualquier medio» (Arocena, 2012, pp. 950-951).

Para entender lo mencionado, nos debemos referir al tratamiento automatizado de datos que no es otra cosa que la labor mecánica que realiza el dispositivo electrónico manejado por una persona física.

En la década de los noventa, la globalización, impulsada por los avances en tecnología y medios de comunicación, inició un proceso de expansión mundial. Este fenómeno se debió principalmente al surgimiento y popularización de Internet. El vocablo «*internet*»

[7] La canción «*Imagine*» (Lennon, 1971), proveniente del álbum homónimo, es reconocida como una de las obras más populares e influyentes grabadas por John Lennon tras la disolución de The Beatles. Esta pieza, concebida e interpretada por el músico inglés, con letras coescritas junto a Yoko Ono a principios de 1971, propone una visión de un mundo sin fronteras ni divisiones, promoviendo la paz y la fraternidad universal.

[8] Real Academia Española. (2001). Informática. En Diccionario de la lengua española. Recuperado el 15 de mayo de 2024, de https://www.rae.es/drae2001/inform%C3%A1tica

es de uso común dentro de la sociedad, cualquier persona sabe y conoce de qué se trata cuando su expresión resuena en sus oídos. No obstante, debido a su relevancia en la sociedad el Diccionario de la Real Academia Española define al término internet como la «*red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación*»[9].

Las ventajas y desventajas fueron advertidas originariamente en Europa, y posteriormente en la Latinoamérica. Los Estados, entre los que se distinguen Alemania, Canadá, Estados Unidos, Francia, Italia, Japón, Reino Unido y Rusia comenzaron a discutir sobre la delincuencia ciberespacial, y para delimitar las fronteras punitivas a tratar acuñaron la alocución «*delitos informáticos*», haciendo referencia a cualquier conducta ilícita ejecutada a través del uso de las redes informáticas (González, Bermeo, Villacreses & Guerrero, 2018).

En el Convenio sobre Ciberdelitos de Budapest (23/11/2001), en el Capítulo: «*terminologías*», se expresaron las siguiente definiciones: a) «*sistema informático*»: será todo dispositivo aislado o conjunto de dispositivos interconectados o unidos, que aseguran, en ejecución de un programa, el tratamiento automatizado de datos; b) «*datos informáticos*»: será toda representación de hechos, informaciones o conceptos expresados bajo una forma que se preste a tratamiento informático, incluido un programa destinado a hacer que un sistema informático ejecute una función; c) «*prestador de servicio»:* será por un lado, toda entidad (pública o privada) que ofrezca a los usuarios sus servicios otorgando la posibilidad de comunicar a través de un sistema informático, por otro lado, cualquier otra entidad que trate o almacene datos informáticos para ese servicio de comunicación de sus usuarios; d) «*datos de tráfico*»: serán todos los datos que tienen relación con una comunicación por medio de un sistema informático, producidos por este último, en cuanto elemento de la cadena de comunicación, indicando el origen, el destino, el itinerario, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente (art. 1).

Aclarando estas nociones generales, debemos señalar que las modalidades delictivas se darán en el campo de las Tecnologías de la Información y la Comunicación (TIC). Las denominadas TIC son el conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones (app), redes y medios que admiten la compilación, procesamiento, almacenamiento y transmisión de información.

Según Aboso (2014) se ha distorsionado la categorización de los delitos informáticos, por ende, existe una aplicación errada de su conceptualización en la doctrina y jurisprudencia. Señala que, en esta categoría únicamente entran aquellas conductas caracterizadas por el empleo abusivo de una terminal que provoca daños económicos a terceros, o bien que consiente el ingreso ilegítimo a una base de datos, o también quien introduce un virus en el sistema informático. Para el mencionado autor esta noción es imprecisa y ambigua, ya que ciñe el término «*delitos informáticos*» a cualquier acontecimiento delictivo relacionado con la utilización de una terminal (dispositivo electrónico que se utiliza para interactuar con un computador).

Bajo esta perspectiva restringida del concepto de delitos informáticos se pretende generar una autonomía funcional en los citados ilícitos cibernéticos. Se destaca que los delitos informáticos tienen como características menoscabar la intimidad personal y la

[9] Real Academia Española. (2001). Internet. En Diccionario de la lengua española. Recuperado el 11 de mayo de 2024, de https://dle.rae.es/internet

propiedad de terceros. Se puede deducir que las conductas ilícitas comprendidas son el ingreso ilegítimo a una base de datos, la utilización no autorizada de un ordenador, la destrucción de un sistema informático, la eliminación de la información almacenada a través del empleo de un virus o la interrupción temporal de dicho servicio, etc. (Aboso & Zapata, 2006).

Por su parte, el autor Flores Cáceres (2023) comparte la conceptualización de Morillas Fernández, quien adopta una tesis restrictiva, ya que considera que el vocablo delito informático debe hacer referencia a

> «[…] cualquier acto ilegal que requiere del conocimiento de la tecnología informática para su perpetración, investigación y persecución, de tal forma que el empleo mismo del medio informático caracterice a la conducta, brindándose así una valoración autónoma al delito informático que le permite su diferenciación respecto de un ilícito penal común que utilice como medio de comisión a la computadora» (p. 89).

En una visión opuesta se encuentra Arocena (1997), quien considera que los delitos informáticos son aquellas modalidades criminales que usan un sistema informático como medio para la perpetración de distintos ilícitos, como cuando dicho sistema informático se transforma en el objeto de ataque.

En síntesis, para el autor Arocena (2012), el delito informático

> «[…] 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 aquellos, en parte o en todo, como su objeto, se vinculan con el tratamiento automático de datos» (p. 950).

Como se puede observar, existe también una perspectiva amplia sobre la conceptualización de los delitos informáticos, en la cual se coloca el foco no tanto en la protección del sistema informático en sí, sino en la modalidad delictiva producida en el ciberespacio. En definitiva, el concepto de delito informático (y/o ciberdelito) se construye alrededor del término «*sistema informático*», ya sea que dicho sistema informático sea el instrumento del delito (medio elegido por el autor a través del cual se ejecuta la acción típica), o bien su objeto de ataque (centro material sobre el cual se asienta la conducta típica del autor).

Una característica esencial de los delitos informáticos es su extraterritorialidad y su intemporalidad[10]. Se podría decir que no existen fronteras y que la delincuencia se ha globalizado, es decir, no es necesario que el autor del ilícito resida en el mismo territorio a la hora de efectuar la conducta criminal. La delincuencia cibernética actúa generalmente escondiendo su identidad y/o rostro, así como su accionar lesivo. Dichas conductas son llevadas a cabo por sujetos que actúan bajo un manto de impunidad y sobre seguro (sin

[10] Al respecto, señala Arocena (2012) que, acorde al artículo 1 del Código Penal se aplica en lo referente a la validez espacial de la ley penal el principio de territorialidad, por ende, únicamente resultará aplicable de forma subsidiaria el principio real, de defensa o de protección del Estado.
En efecto, señala el Prof. Domínguez Henaín (s.f.) que la regla general es la territorialidad de la ley penal argentina respecto de las causas criminales; es decir, que este principio resulta aplicable a todos aquellos delitos cometidos dentro del territorio nacional. Ahora bien, cuando la norma del artículo 1 del Código Penal hace alusión al «territorio», esta no debe interpretarse en un sentido meramente geográfico, sino en un sentido jurídico. La redacción legal no es del todo clara y, en este contexto, se discute cómo debe interpretarse la expresión «lugar de comisión del delito» y de qué manera deben resolverse los casos denominados «delitos a distancia».

riesgo de ser atrapados por el sistema penal) producto de la propia naturaleza del ciberespacio.

Para esta posición, el sistema informático (y/o toda fuente de transmisión de datos) puede ser el medio para cometer otros delitos, por ejemplo: la tenencia de pornografía infantil con fines inequívocos de distribución o comercialización (art. 128, 3° párr., CP)[11]; el delito de grooming (art, 131, CP)[12]; entre otros. Así como también puede ser directamente el sistema informático el centro de la agresión, así verbigracia: el delito de acceder ilegítimamente a un sistema o dato informático de acceso restringido (art. 153 bis, CP)[13]; el delito de daño informático (art. 183, 2° párr., CP)[14], etc.

Por otra parte, la doctrina ha clasificado los delitos informáticos según el objeto de protección. Si el bien jurídico afectado se vincula con los datos o información automatizada a la que se accede de modo no autorizado, los llama delitos informáticos propios. En cambio, son delitos informáticos impropios aquellos en los que la informática es utilizada como medio para la comisión de un delito distinto de aquel de acceso no autorizado (Garibaldi, 2014).

En el derecho comparado, se han adoptado tres sistemas para regular los delitos informáticos dentro de un Código Penal, entre las que se destacan: 1) las legislaciones que lo hacen a través de una ley especial referida a la informática y tecnologías de la comunicación; 2) Otras legislaciones lo plasman en un título propio y específico dentro de los Códigos Penales; 3) En otra sintonía están las legislaciones penales que tipifican en distintas figuras dispersar en los Códigos Penales. Esta última es la metodología utilizada por el legislador argentino (Arocena & Balcarce, 2015).

Los distintos países han elegido criminalizar las conductas lesivas generadas por la ciberdelincuencia en el ámbito espacial, entre ellos se encuentran Chile, Venezuela y Alemania, quienes utilizaron la mecánica de legislar a través de una ley especial -por fuera del Código Penal- los delitos informáticos que han creído convenientes.

Por otro lado, se puede observar la experiencia legislativa de Bolivia, quien reguló las figuras penales vinculadas a los delitos informáticos en un capítulo único, dentro del título de los delitos contra la propiedad en el Código Penal. En cambio, en sentido similar a nuestro país se encuentran España, Paraguay y Francia, quienes legislaron los delitos informáticos dentro del Código Penal, pero no en un título y/o capítulo único, sino que los tipos penales están diseminados por todo el texto legal.

---

[11] Artículo 128: «Será reprimido con prisión de seis (6) meses a dos (2) años el que tuviere en su poder representaciones de las descriptas en el primer párrafo con fines inequívocos de distribución o comercialización».

[12] Artículo 131: «Será penado con prisión de seis (6) meses a cuatro (4) años el que, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contactare a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma».

[13] Artículo 153 bis: «Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el 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. La pena será de un (1) mes a un (1) año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros».

[14] Artículo 183: «Será reprimido con prisión de quince (15) días a un (1) año […]. En la misma pena incurrirá el 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».

4. Hacia una definición y clasificación de los delitos informáticos

El Código Penal argentino no brinda una definición conceptual de delitos informáticos, por lo tanto, tampoco los clasifica dentro del catálogo de los delitos regulados en dicho Código. En los últimos años, la doctrina se ha encargado de formular distintas conceptualizaciones de delito informático, así como una clasificación que lo diferencia del delito común. Al principio, la importancia parecía ser puramente teórica, pero a medida que las investigaciones en el campo fueron avanzando, se dieron cuenta de que fijar cuándo estamos frente a un delito informático resulta indispensable desde el punto de vista práctico.

Como se ha dicho, es indispensable precisar un concepto de delito informático desde el punto de vista práctico, puesto que, por ejemplo, permite poder identificar, investigar y sancionar de manera eficaz a aquellas acciones que vulneran la seguridad de la información en entornos digitales, así como también bienes jurídicos personales (honor, libertad sexual, patrimonio, intimidad, etc.). Una enunciación clara de delito informático ayudará a la prevención de futuras transgresiones en el ciberespacio de bienes jurídicos individuales y colectivos.

Determinar los distintos tipos de delitos informáticos existentes es relevante, pues proporciona un instrumento de vanguardia en el ámbito de la seguridad informática para enfrentar de manera efectiva las consecuencias personales, económicas y sociales que surgen al ser víctimas de estos actos delictivos. Al mismo tiempo, resulta esencial conocer los riesgos que implica confiar información de carácter personal, financiero y/o empresarial a sitios o aplicaciones que pueden ser transgredidos ilícitamente por delincuentes cibernéticos, tales como hackers, crackers, phrackers y piratas informáticos. Esto permite a los usuarios protegerse de convertirse en víctimas de fraude, extorsión, chantaje, entre otros delitos. (Acosta, Benavides & García, 2020).

En este sentido, considero que los delitos informáticos pueden ser conceptualizados como aquellas conductas típicas, antijurídicas y culpables que lesionan un sistema informático y/o sistema de transmisión de datos informáticos, así como también aquellas conductas ilícitas donde el sistema informático resulta central como medio para lesionar otros bienes jurídicos.

Por lo tanto, desde el punto de vista clasificatorio estaremos en presencia de un delito informático de carácter propio cuando el objeto de agresión es el sistema informático en sí. En cambio, será un delito informático impropio cuando el sistema informático sea el medio idóneo y especial para lesionar otros bienes jurídicos.

Cabe aclarar que el mero uso de la tecnología no transforma una figura penal clásica en un delito informático. Por ejemplo, delitos como el homicidio, las lesiones o la privación de libertad no se convierten en delitos informáticos simplemente por involucrar tecnología en su ejecución. En este sentido, la simple intervención de un sistema informático por sí sola no permite catalogar al tipo penal como delito informático.

Para ejemplificar lo mencionado, consideremos un caso de privación de la libertad. Supongamos que el delincuente no proporciona a la víctima los datos necesarios para acceder al sistema informático que controla el sistema de seguridad del domicilio, impidiendo así que la víctima pueda salir del lugar. Aunque hay un componente

tecnológico en la comisión del delito, el acto principal sigue siendo la privación de libertad, no un delito informático per se.

Estaremos en presencia de un delito informático cuando la intervención a través de un sistema informático sea el medio fundamental para alcanzar el fin delictivo. Este medio debe ser de tal intensidad que no pueda dejar de considerarse como un elemento objetivo esencial para la ejecución y/o consumación del tipo penal. De esta manera, la informática tiene que ser el medio imprescindible e indispensable para cometer el ilícito penal.

Para ilustrar este punto, basta referirnos al delito de «*grooming*». Según el art. 131 del Código Penal argentino, será castigado con prisión de seis (6) meses a cuatro (4) años quien, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contacte a una persona menor de edad con el propósito de cometer cualquier delito contra su integridad sexual. Como se puede advertir, la informática es un medio fundamental para perpetrar esta infracción penal, situación que amerita una investigación especializada en delitos informáticos.

Como corolario, resulta conveniente acorde a la política criminal que nuestro país ha adoptado para prevenir, investigar, sancionar y erradicar conductas ejecutadas y desarrolladas por ciberdelincuentes en el ciberespacio definir a los delitos informáticos como aquellos ilícitos cometidos a través de la informática, relativos -entre otros- a la intimidad, la libertad, la indemnidad sexual, etc. Necesariamente esta conceptualización abarca a los denominados delitos informáticos propios e impropios.

5. El estado actual de los delitos informáticos en el Código Penal argentino

La globalización de la tecnología trajo aparejadas ventajas, como la multiplicidad de información mundial y la comunicación instantánea con las personas de manera ilimitada. Ahora bien, también trajo consigo desventajas, entre ellas, se facilitó la comisión de delitos, sin mostrar el rostro del delincuente, con el consecuente menor poder de defensa de la víctima, daños a los sistemas informáticos y de datos, violación a la intimidad y privacidad, entre otras conductas inapropiadas para una vida en sociedad.

En una sociedad de riesgo se encuentra el uso abusivo de los ordenadores por los individuos (riesgo permitido), es decir, esta conducta genera constantemente un peligro concreto y efectivo desde el punto de vista cuantitativo y cualitativo para las personas. Esta situación se debe a la dependencia que tienen las personas a la operatividad cotidiana y necesaria que se hace de los sistemas informáticos. Por ejemplo: aplicaciones en celulares (Instagram, Facebook, WhatsApp, etc.) para conectarse de inmediato con otras personas; las empresas ya tienen sistemas automatizados e informatizados que permiten solucionar cuestiones empresariales y adoptar respuestas efectivas a los problemas cotidianos; hoy la mayoría de las transacciones económicas y financieras se hacen a través de plataformas informatizadas (home banking) instaladas en un celular, tablet o computadora.

La política criminal de un país debe estar ocupada en situaciones como las descritas, y para ello debe adoptar medidas preventivas, así como también represivas, si fuera necesario, al margen de la obligación internacional que como Estado se haya obligado a cumplir.

Nuestro país legisla sobre los delitos informáticos en diferentes artículos del Código Penal. En este contexto, se ha señalado que el «internet es el instrumento que justifica desde una perspectiva político-criminal un tratamiento diferenciado, tanto por el Derecho Penal material como por el procesal» (Morabito, 2011, p. 1).

En términos generales, en el Código Penal de la Nación existen delitos informáticos contra la libertad sexual, indemnidad sexual de los menores de edad (niños, niñas y adolescentes), libertad individual, propiedad (patrimonio), seguridad pública y Administración Pública[15].

6. Propuesta de reforma al Código Penal: «*delitos informáticos*»

No resulta sencillo adherirse a una u otra conceptualización y clasificación de los delitos informáticos, especialmente porque sostener una u otra tesis sobre la noción del mismo puede generar distintas consecuencias prácticas.

En este análisis que estamos realizando es ilustrativo observar qué posturas adoptaron los últimos Anteproyectos de Código Penal de la Nación en Argentina, así como también qué metodología utilizaron y si verdaderamente incorporaron una definición de delito informático.

Recordemos que nuestro actual Código Penal de Nación no brinda una definición de delito informático, ni tampoco de sistema informático, dato informático o información. Por otro lado, hoy incluye algunos delitos que castigan la cibercriminalidad, ya sea cuando el sistema informático es el objeto de agresión, o bien cuando la informática es el instrumento para cometer otro delito. Dichas figuras penales se encuentran desconcentradas por todo el texto penal, es decir, no se prefirió concentrar los delitos informáticos en un título o capítulo exclusivo.

En el año 2014, se difundió el Anteproyecto de Código Penal del Dr. Raúl. E. Zaffaroni (Director) y un cuerpo especializado al efecto. En dicho texto se establecen los significados de sistema informático y datos informáticos[16]. No define qué es delito informático ni sus sinónimos (ciberdelitos, etc.). Por otro lado, adopta la postura de no legislar en un título único los delitos informáticos, sino que lo realiza de forma dispersa, es decir, que incorpora las figuras delictivas (acceso ilegítimo a información en sus diferentes modalidades; daño informático; etc.) en distintos títulos del Código. En líneas generales, sigue la metodología usada por el actual Código Penal argentino.

Por su parte, en el año 2018 surge a divulgación el Anteproyecto de Código Penal del Dr. Mariano H. Borinsky (Director) acompañado también por un grupo de especialistas

[15] Véanse las Leyes N.º 25.930, N.º 26.388, N.º 26.904 y N.º 27.436.

[16] En el «*Anteproyecto de Código Penal de la Nación*» (2014), Título X, bajo el artículo 63 —«*Significación de Conceptos Empleados en el Código*»— se establecen las siguientes definiciones: «(…) s) Por 'sistema informático' se entiende 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. t) «Dato informático» es toda representación de hechos, información o conceptos expresados de cualquier forma, que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función. El término comprende, además, los datos relativos al tráfico, entendiendo como tales todos los relativos a una comunicación realizada por medio de un sistema informático, generados por este último en tanto que elemento de la cadena de comunicación, y que indican el origen, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente».

del ámbito penal. En este cuerpo normativo se observa una gran novedad al respecto, ya que cambia la tradicional metodología de regular los delitos informáticos. En este sentido, se instituye un título dedicado exclusivamente a los ciberdelitos (Título XXVI: «*delitos informáticos*», arts. 491 a 503). En consecuencia, adopta el método de sistematizar los delitos informáticos en un solo título, es decir, agrupa todos los delitos informáticos propiamente dichos (Capítulo 1: Atentados a través de Medios Informáticos; Capítulo 2: Daño Informático; Capítulo 3: Hurto y Fraude Informáticos; Capítulo 4: Acceso Ilegítimo; y Capítulo 5: Disposiciones Generales).

Al margen de este método (agrupamiento de todos los delitos informáticos en un título único) usado por la Comisión Redactora del Anteproyecto, se advierte que adhieren a la clasificación de delitos informáticos propios e impropios, así como además a una conceptualización amplia del mismo. En este sentido, se reprime la suplantación de identidad con la intención de cometer un delito o causar un perjuicio a la persona cuya identidad se suplanta o a terceros (art. 492) y también la «*pornovenganza*» (art. 493)[17].

Sin embargo, ha señalado con razón Riquert (2019) que si bien se ha incorporado un título específico para los «*delitos informáticos*», se puede advertir que se ha provocado como consecuencia que numerosos tipos penales han permanecido en su ubicación actual, por lo que puede pensarse que la concentración que el título propone no es en realidad tal y que las normas de interés permanecen, al menos parcialmente, desechadas o distribuidas en otros títulos.

7. Conclusión final

Se han explicado las diversas definiciones y clasificaciones de los delitos informáticos con el fin de alcanzar una noción conceptual uniforme en el derecho penal argentino. Se ha efectuado un relevamiento de la normativa nacional e internacional sobre los delitos informáticos, lo cual es particularmente valioso dado que el Código Penal argentino no define ni dedica un título específico a las infracciones cibernéticas.

Por otra parte, existen dos posturas que son similares en algunos aspectos y antagónicas en otros en relación con la precisión conceptual del delito informático. Dichas posturas coinciden en que estamos en presencia de un delito informático cuando el objeto de agresión es un sistema informático y/o dato informático. Sin embargo, difieren cuando la informática es el medio para cometer otro u otros delitos.

Consideramos que el concepto de delito informático (o ciberdelito) gira en torno al término «*sistema informático*». Este sistema puede actuar de dos maneras distintas: como el medio mediante el cual se ejecuta la acción delictiva, o como el objetivo del ataque. En otras palabras, el sistema informático puede ser el instrumento que utiliza el autor del

[17] Asimismo, el «*Anteproyecto de Código Penal de la Nación*» (2018) incorpora, en su artículo 493, la tipificación de la denominada «pornovenganza» (o «*porn revenge*»), con una pena para el tipo básico de seis (6) meses a dos (2) años de prisión y días multa. La norma establece que: «el que, sin autorización de la persona afectada, difunda, revele, envíe, distribuya o de cualquier forma ponga a disposición de terceros imágenes, grabaciones de audio o audiovisuales de naturaleza sexual, producidas en un ámbito de intimidad, que el autor hubiera recibido u obtenido con el consentimiento de la víctima, cuando la divulgación menoscabe gravemente su privacidad». Asimismo, se prevén agravantes —reprimidas con una pena de uno (1) a tres (3) años de prisión— cuando los hechos hubieran sido cometidos por una persona que esté o haya estado unida a la víctima por matrimonio o análoga relación de afectividad, aun sin convivencia; si la víctima fuera menor de edad; o si los hechos se hubieran cometido con fines de lucro.

delito para llevar a cabo la acción típica, o bien el objeto material sobre el cual se dirige su conducta delictiva. Esta conceptualización abarca la clasificación de los delitos informáticos propios e impropios.

Para concluir, este trabajo no solo ha tenido una finalidad teórica, sino también práctica. Su objetivo ha sido proporcionar una comprensión conceptual de los delitos informáticos según el Código Penal argentino, delimitando su alcance y contenido para orientar la competencia necesaria en la investigación penal especializada.

Como se ha destacado, es fundamental distinguir entre un delito ordinario y un delito informático. Identificar correctamente la naturaleza y el tipo de delito informático permite, entre otras cosas: 1) que la investigación y/o recolección de evidencia digital sea llevada a cabo por organismos especializados en el área (campo informático), como fiscalías y fuerzas de seguridad especializadas en ciberdelitos; 2) que se utilicen herramientas ceñidas para garantizar una adecuada seguridad informática; y 3) que se asegure la intimidad, privacidad y datos de la presunta víctima, entre otros.

8. Referencias bibliográficas

Aboso, G. & Zapata, M. F. (2006). Cibercriminalidad y derecho penal. Buenos Aires: B de F.

Aboso, G. E. & Buompadre, J. E. (2015). El derecho penal y procesal penal frente a los retos del tercer milenio (1.ª ed.). Resistencia: Contexto Libros.

Aboso, G. E. (2014). «El delito de contacto telemático con menores de edad con fines sexuales. Análisis del Código Penal argentino y del Estatuto da Criança e do Adolescente brasileño». Revista Derecho Penal, Año III, N.º 7, Ministerio de Justicia y Derechos Humanos de la Nación.

Acosta, M. G., Benavides, M. M. & García, N. P. (2020). «Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios». Revista Venezolana de Gerencia, 25(89), 1–15. Recuperado el 26/04/2024 de https://www.redalyc.org/journal/290/29062641023/29062641023.pdf

Arocena, G. A. & Balcarce, F. I. (2015). «Child grooming. Contacto tecnológico con menor para fines sexuales». En Aboso, G. E. & Buompadre, J. E. (comps.), El derecho penal y procesal penal frente a los retos del tercer milenio (1.ª ed.). Resistencia: Contexto Libros.

Arocena, G. A. (1997). «De los delitos informáticos». *Revista de la Facultad de Derecho*, Universidad Nacional de Córdoba, 5(1).

Arocena, G. A. (2012). «La regulación de los delitos informáticos en el Código Penal argentino. Introducción a la Ley Nacional N.º 26.388». Boletín Mexicano de Derecho Comparado, 45(135), 945–988.

Buompadre, J. E. (2015). Grooming: Una nueva forma de acoso sexual a menores en el mundo (1.ª ed.). Resistencia: Contexto Libros.

Domínguez Henaín, D. H. (s.f.). Módulos de Derecho Penal. Parte General. Corrientes.

Flores Cáceres, J. H. (2023). «Delitos a través de plataformas virtuales. ¿Vinculación necesaria a los tipos penales previstos en la Ley de Delitos Informáticos?». En

Espinoza Calderón, V. R. (ed.), Cibercriminalidad y delitos informáticos (1.ª ed.). Perú.

Garibaldi, G. E. L. (2014). «Aspectos dogmáticos del grooming legislado en Argentina». Revista Derecho Penal, Año III, N.º 7, Ministerio de Justicia y Derechos Humanos de la Nación.

González Tascón, M. (2011). «El nuevo delito de acceso a niños con fines sexuales a través de las TIC». Estudios Penales y Criminológicos, XXXI, 207–258.

González, J., Bermeo, J., Villacreses, E. & Guerrero, J. (2018). «Delitos informáticos: Una revisión en Latinoamérica». Conference Proceedings UTMACH, 2(1), mayo.

Morabito, M. R. (2011). «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, Suplemento de Actualidad, 07/06/2011.

Riquert, M. A. (2019). «Las propuestas del Anteproyecto de Código Penal de 2018 en materia de delincuencia informática». Revista Pensamiento Penal. Recuperado el 01/07/2024 de https://www.pensamientopenal.com.ar/doctrina/47358-delitos-informaticos-anteproyecto-codigo-penal-2018

Temperini, M. (2018). «Delitos informáticos y cibercrimen: Alcances, conceptos y características». En Suplemento Especial Cibercrimen y Delitos Informáticos. Los nuevos tipos penales en la era de internet. ERREIUS, 49–68.

Villacampa Estiarte, C. (2014). «Propuesta sexual telemática a menores u online child grooming: Configuración presente del delito y perspectivas de modificación». Estudios Penales y Criminológicos, XXXIV, 639–712.

Zaffaroni, E. R., Slokar, A. & Alagia, A. (2002). Derecho penal: Parte general. (2.ª ed.). Buenos Aires: Ediar.

Leyes y documentos legales:

Anteproyecto de Código Penal de la Nación. (2014).

Anteproyecto de Código Penal de la Nación. (2018).

Código Penal de la Nación.

Ley N.º 25.930 de Modificación del Código Penal de la Nación. (2004).

Ley N.º 26.388 de Modificación del Código Penal de la Nación. (2008).

Ley N.º 26.904 de Modificación del Código Penal de la Nación. (2013).

Ley N.º 27.411 de Aprobación del Convenio sobre Ciberdelito. (2017).

Ley N.º 27.436 de Modificación del Código Penal de la Nación. (2018).