DELITOS INFORMATICOS, CIBERCRIMEN Y EVIDENCIA DIGITAL

Natalia Molina Areal [1]

RESUMEN

El presente artículo examina los delitos informáticos y el cibercrimen desde una perspectiva multinivel: internacional (Convenio de Budapest), nacional (legislación argentina) y provincial (Santiago del Estero).

Se distingue conceptualmente entre delitos informáticos —conductas individuales— y cibercrimen —delincuencia organizada con fines económicos, presentando una clasificación según el Ministerio de Justicia argentino.

El trabajo problematiza los desafíos de la evidencia digital, caracterizada por volatilidad, duplicabilidad y alterabilidad, que demanda técnicas específicas de recolección y preservación. Se abordan cuestiones críticas como los límites del ciberpatrullaje frente al derecho a la intimidad, la necesidad de reformas procesales que regulen la investigación en entornos digitales, y la importancia de fortalecer los mecanismos de cooperación internacional.

El análisis se nutre de casos prácticos de Santiago del Estero, evidenciando avances y deficiencias del sistema argentino para enfrentar esta criminalidad compleja y transnacional. Se concluye en la necesidad impostergable de reformas legislativas, capacitación especializada e inversión en tecnología forense.

---

[1] **Natalia Molina Areal**, abogada (Universidad Católica de Santiago del Estero); Diplomada en Derecho Procesal Penal (Universidad Austral); Especialista en Derecho Penal (Universidad Nacional de Rosario) y Maestranda en Derecho Penal (Universidad Austral).

Palabras clave: delitos informáticos, cibercrimen, evidencia digital, Convenio de Budapest, investigación penal, ciberpatrullaje, cooperación internacional.

SUMARIO

INTRODUCCIÓN

El presente trabajo tiene por finalidad abordar el estudio de los nuevos delitos, llamados en doctrina «informáticos», a la vez que analiza el cibercrimen y la investigación en entornos digitales, tanto a nivel internacional, mediante el análisis del Convenio sobre Cibercrimen, firmado en la Ciudad de Budapest, Hungría, como a nivel de derecho interno, en lo que respecta a la legislación de fondo y de forma, a través del análisis de las leyes vigentes en Argentina y el sistema que rige en la Provincia de Santiago del Estero, de la cual soy oriunda.

A modo introductorio, podemos decir que no correspondería afirmar que los delitos informáticos son un «nuevo fenómeno», al menos socialmente. Sí podríamos aceptar que es algo «nuevo» para el derecho, particularmente, para el derecho penal.

---

[1] **Natalia Molina Areal**, abogada (Universidad Católica de Santiago del Estero); Diplomada en Derecho Procesal Penal (Universidad Austral); Especialista en Derecho Penal (Universidad Nacional de Rosario) y Maestranda en Derecho Penal (Universidad Austral).

La delincuencia informática lleva varios años de gestación, desarrollo, y sobre todo de mucha práctica, bastante lucrativa para los delincuentes, pero, no deja de sorprender que, en la última década, el índice de ciberdelincuencia haya aumentado notoriamente (y más aún, con el surgimiento de la pandemia por Covid-19); o quizás, es una problemática que, a los ojos del ciudadano común, se ha hecho cada vez más visible.

Con el advenimiento del fenómeno informático se ha originado una revolución en todo el mundo, lo que nos permite afirmar que estamos siendo protagonistas de una nueva era, llamada «informática» o «digital», en la que la tecnología de la información y de las telecomunicaciones, ha avanzado, y avanza, a pasos agigantados.

Al igual que la tecnología, la delincuencia también ha cambiado. Se ha modernizado. Así, se emplean herramientas tecnológicas sofisticadas para la comisión de delitos, pues el perpetrador busca ocultar su identidad (anonimato) y asegurar sus objetivos.

Si bien el avance de la tecnología ha contribuido a un enorme desarrollo económico, social y político, y ha dado lugar a cambios sin precedentes, como la posibilidad de la comunicación instantánea, el contacto a distancia, la posibilidad de teletrabajo, acceso a la información, etc., al mismo tiempo, tiene un lado negativo, caracterizado por el surgimiento de nuevos tipos de delitos, a los que, en doctrina, se ha denominado «Delitos Informáticos».

Estos delitos, cometidos en el ciberespacio, abarcan tanto, actividades que atentan contra la integridad, la disponibilidad y la confidencialidad de los sistemas informáticos y las redes de telecomunicaciones, como el uso de esas

---

[1] **Natalia Molina Areal**, abogada (Universidad Católica de Santiago del Estero); Diplomada en Derecho Procesal Penal (Universidad Austral); Especialista en Derecho Penal (Universidad Nacional de Rosario) y Maestranda en Derecho Penal (Universidad Austral).

redes o sus servicios para cometer «Delitos Tradicionales», en los cuales los ordenadores y las redes han sido utilizados como medio.

Las consecuencias de estas conductas delictivas, hoy, pueden tener un mayor alcance que antes, porque no están restringidas por límites geográficos ni fronteras, lo que implica que cualquier delincuente informático puede ejecutar acciones desde un determinado país, conectándose a sistemas o equipos en otro, y finalmente atacar datos o sistemas ubicados en un tercer país, por lo que encontramos autores, víctimas y evidencias dispersas por todo el mundo: la cadena puede tener indeterminadas variables, dependiendo de la complejidad del ataque y de los conocimientos del delincuente.

Todo ello conduce a una mayor dificultad para la investigación de estos delitos, a los que podemos caracterizar como «complejos», y obstaculiza, al mismo tiempo, la obtención de elementos de prueba, lo que, a mi parecer, resulta cada vez más atractivo para aquellas personas u organizaciones que se «dedican» a delinquir, sabiendo que pueden actuar con más rapidez y en anonimato, y es por ello que cada día crece más el porcentaje de los delitos que motivan el presente trabajo.

Los delitos informáticos, como todo fenómeno relacionado con las nuevas tecnologías, son una problemática de índole internacional o general, donde los límites jurisdiccionales clásicos del derecho suelen tornarse cada vez más borrosos. Esto afecta al principio de territorialidad, y genera conflictos en materia de jurisdicción de las autoridades nacionales encargadas de imponer el cumplimiento de las leyes, lo que demuestra que resulta fundamental un esfuerzo y cooperación internacional, reforzada, rápida y eficaz en materia penal, para hacer frente a ese uso impropio de la tecnología, e incrementar la eficacia de las investigaciones y procedimientos penales relativos a sistemas y datos

---

[1] **Natalia Molina Areal**, abogada (Universidad Católica de Santiago del Estero); Diplomada en Derecho Procesal Penal (Universidad Austral); Especialista en Derecho Penal (Universidad Nacional de Rosario) y Maestranda en Derecho Penal (Universidad Austral).

informáticos, así como para permitir la obtención de pruebas electrónicas de estos delitos.

La investigación en entornos digitales se ha vuelto todo un desafío para la justicia, tanto a nivel nacional como internacional, sobre todo, a mi modo de ver, en países subdesarrollados que no cuentan con las herramientas y/o recursos necesarios para acceder a cierto tipo de evidencias, lo que muchas veces conduce, o puede conducir, a la «impunidad» de las personas responsables, y no solo me refiero a recursos materiales o técnicos, sino también a recursos humanos, es decir, a personas capacitadas para investigar estas conductas delictivas tan complejas.

En consecuencia, me surgen los siguientes interrogantes: **¿en Argentina, estamos capacitados para enfrentarnos a estas nuevas modalidades delictivas? ¿destinamos recursos para capacitar personal e invertir en herramientas que nos faciliten el acceso y análisis de este nuevo tipo de evidencia, llamada evidencia digital?** Interrogantes que, a partir de la información recopilada, trataré de responder a lo largo de mi exposición.

---

1. DELITOS INFORMÁTICOS Y CIBERCRIMEN

Inicialmente, debemos reconocer la inexistencia de un acuerdo en la doctrina acerca de la definición de los delitos informáticos. Una de las primeras dificultades a la hora de afrontar el análisis de los mismos es su conceptualización. No obstante, corresponde indicar que los delitos de informática son producto de la criminalidad evolutiva, la cual nace concomitantemente con las nuevas tecnologías informáticas y telemáticas, y delito informático, es aquel que se comete con el empleo de computadoras o

---

[1] **Natalia Molina Areal**, abogada (Universidad Católica de Santiago del Estero); Diplomada en Derecho Procesal Penal (Universidad Austral); Especialista en Derecho Penal (Universidad Nacional de Rosario) y Maestranda en Derecho Penal (Universidad Austral).

equipos electromagnéticos que transmiten datos o información. Según Tiedemann, delitos informáticos alude a todos los actos antijurídicos según la ley penal vigente (o socialmente perjudiciales y por eso penalizables en el futuro), realizados con el empleo de un equipo automático de datos.

Existen diferencias entre el concepto de delitos informáticos y cibercrimen, los que normalmente son utilizados como sinónimos, pero que, a fines académicos y doctrinarios, no son lo mismo. Principalmente, la diferencia radica en la organización del delito. Es decir, cuando referimos a delitos informáticos, nos referimos a aquellos delitos 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. Bastaría dar como ejemplo un caso de acceso indebido a una cuenta de correo electrónico, por ejemplo, realizado por una pareja a su ex pareja; o bien, un empleado enojado que borra información importante de la empresa a la que pertenece. El denominador común de estos casos es que los delitos existen y ocurren, pero se cometen o llevan a cabo, de forma aislada o independiente.

En cambio, cuando referimos al cibercrimen, estamos hablando de una serie de delitos informáticos que ocurren de una forma más profesional, organizada, sin motivaciones personales más que las económicas, donde 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. Como ejemplo en casos de cibercrimen, podemos mencionar el ransomware, un tipo de malware (software malintencionado) que tiene como objetivo bloquear el acceso a toda o parte de la información que contiene el equipo, para después pedir un rescate a cambio de su liberación. Advertimos, que los ciberdelincuentes no están interesados en el objetivo o en la víctima, en

---

[1] **Natalia Molina Areal**, abogada (Universidad Católica de Santiago del Estero); Diplomada en Derecho Procesal Penal (Universidad Austral); Especialista en Derecho Penal (Universidad Nacional de Rosario) y Maestranda en Derecho Penal (Universidad Austral).

su información en particular, sino que se realiza de forma masiva, buscando un fin de lucro, que es el pago por el rescate. Es un negocio organizado, donde las bandas suelen estar compuestas por muchas personas que se dividen tareas, y en donde, por supuesto, hay líderes.

Si bien es posible encontrar ciberdelincuentes especializados que trabajan de forma independiente, es mucho más común encontrarlos organizados en bandas, con una clara distribución de tareas.

Según la clasificación brindada por el Ministerio de Justicia y Derechos Humanos de la Nación Argentina, podemos agrupar a los ciberdelitos en tres categorías, a saber:

a) Delitos que se cometen a través de programas maliciosos desarrollados para borrar, dañar, deteriorar, hacer inaccesibles, alterar o suprimir datos informáticos sin autorización y con fines económicos y de daño, como ser:

1. Ataques en la navegación: en los que se desvía el navegador hacia páginas que causan infecciones con programas malignos como virus, gusanos y troyanos. Estos programas pueden borrar un sistema operativo, infectar un teléfono y computadora, activar la webcam, extraer datos, etc.
2. Ataques a servidores: a través de los cuales se pueden dañar o robar datos de una persona y negarle el acceso a su información.
3. Corrupción de bases de datos: que son los que interfieren en bases de datos públicas o privadas para generar datos falsos o robar información.
4. Virus informáticos: encriptan archivos, bloquean cerraduras inteligentes, roban dinero desde los celulares con mensajes de texto que parecen de la compañía.

---

[1] **Natalia Molina Areal**, abogada (Universidad Católica de Santiago del Estero); Diplomada en Derecho Procesal Penal (Universidad Austral); Especialista en Derecho Penal (Universidad Nacional de Rosario) y Maestranda en Derecho Penal (Universidad Austral).

5. Programa espía: en los que alguno de los dispositivos tiene instalado un software que le permite encender y grabar con la cámara y el micrófono. También puede acceder a información personal sin autorización y sin que la persona lo sepa.

b) Delitos que usan la ingeniería social para engañar, amenazar y sacar datos personales o información de otras personas u organizaciones, sacarles dinero, suplantar identidad, acosar digital y sexualmente. Algunos ejemplos son:

1. Phishing o Vishing: los ciberdelincuentes se hacen pasar por empresas de servicios, oficinas de gobierno o amigos de algún familiar y piden los datos que les faltan para suplantar una identidad y así operan las cuentas en bancos, perfiles en las plataformas y redes sociales, servicios y aplicaciones web.
2. Ciberbullying: es el acoso por mensajería instantánea, stalking en WhatsApp, Telegram, Messenger, y en las redes sociales, con la intención de perseguir, acechar a otra persona, difamarla, atentar contra su honor e integridad moral. Ello a través del descubrimiento y revelación de secretos, de la publicación de comentarios o videos ofensivos o discriminatorios, la creación de memes o el etiquetado de publicaciones.
3. Grooming: se trata de personas adultas que, de manera velada, intentan obtener fotografías o videos sexuales de personas menores de edad, para posteriores chantajes o previo al abuso sexual.
4. Sextorsión: es una forma de explotación sexual, en la cual una persona (en la mayoría de los casos de sexo femenino) es inducida o chantajeada, generalmente por aplicaciones de mensajería por Internet, con una imagen o video de sí misma desnuda o realizando actos sexuales, mediante sexting. La sextorsión consiste en pedir dinero a cambio de no difundir en las redes, imágenes generadas para un intercambio erótico consentido.

---

[1] **Natalia Molina Areal**, abogada (Universidad Católica de Santiago del Estero); Diplomada en Derecho Procesal Penal (Universidad Austral); Especialista en Derecho Penal (Universidad Nacional de Rosario) y Maestranda en Derecho Penal (Universidad Austral).

5. Ciberodio: son contenidos inapropiados que pueden vulnerar personas. Se considera ciberodio a la violencia, mensajes que incitan al odio, la xenofobia, el racismo y la discriminación o maltrato animal.
6. Pornografía infantil: se trata de la corrupción de personas menores y su explotación sexual para producir, comercializar imágenes y videos de actividad sexual explícita.

c) Delitos que tienen que ver con la violación de la privacidad de las personas:

1. Espionaje ilícito sobre las comunicaciones privadas de los ciudadanos.
2. Violación a la intimidad por parte de las empresas proveedoras de servicios de Internet sin el consentimiento del usuario, para conocer sus gustos y preferencias y establecer la venta agresiva de productos y servicios asociados.
3. Acceso ilegal a las comunicaciones privadas de un trabajador (mails, redes sociales, etc.).

Es importante destacar que este tipo de ilícitos penales son de **difícil represión**, por una serie de circunstancias que los caracterizan, como ser, la falta de una tipificación específica en la mayoría de las legislaciones, la transnacionalidad de las conductas (que muchas veces se realizan en un país, pero cuyos resultados se producen en otro), la falta de consenso internacional sobre su reprochabilidad, las permanentes innovaciones tecnológicas (que generalmente avanzan más rápido que las implementaciones de soluciones normativas), a ello se suma, su instantaneidad, pluriofensividad, masividad, anonimato, la complejidad de su investigación, entre otros.

---

[1] **Natalia Molina Areal**, abogada (Universidad Católica de Santiago del Estero); Diplomada en Derecho Procesal Penal (Universidad Austral); Especialista en Derecho Penal (Universidad Nacional de Rosario) y Maestranda en Derecho Penal (Universidad Austral).

2. LA PROBLEMÁTICA DEL CIBERCRIMEN A NIVEL INTERNACIONAL

La comunidad internacional es totalmente consciente de la existencia de este «fenómeno», y del aumento alarmante de las nuevas modalidades delictivas, es por ello, que el 23 de noviembre del año 2001, durante la celebración de la Conferencia Internacional sobre la Ciberdelincuencia celebrada en la Ciudad de Budapest, Hungría, se abrió a la firma el *Convenio sobre Ciberdelito*, aprobado por el Comité de Ministros del Consejo de Europa, el que entró en vigor el 1 de julio del año 2004, con el objetivo de aplicar una política estatal común para proteger a la sociedad frente a la ciberdelincuencia.

En su preámbulo, el Convenio sobre Ciberdelito establece que los Estados son conscientes de los profundos cambios provocados por la digitalización, la convergencia y la globalización continua de las redes informáticas, destacando su preocupación por el riesgo de que las redes informáticas y la información electrónica, sean utilizadas igualmente para cometer delitos, y que las pruebas relativas a dichos delitos sean almacenadas y transmitidas por medio de dichas redes.

Si bien en su origen, el Convenio fue firmado por pocos países, hoy son más de setenta los que se adhirieron al mismo, siendo el principal instrumento jurídico internacional en materia de ciberdelincuencia, habiéndose dictado dos Protocolos Adicionales. El primero, relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos; el segundo, tiene por objeto afianzar los lazos en materia de cooperación internacional, y facilitar la obtención de evidencia electrónica para brindar una respuesta eficaz en la investigación criminal contra el ciberdelito.

---

[1] **Natalia Molina Areal**, abogada (Universidad Católica de Santiago del Estero); Diplomada en Derecho Procesal Penal (Universidad Austral); Especialista en Derecho Penal (Universidad Nacional de Rosario) y Maestranda en Derecho Penal (Universidad Austral).

Ahora bien, el Convenio de Budapest, impone una serie de medidas - que deberán ser adoptadas a nivel nacional por todos los Estados que se adhieran al mismo- relativas al derecho penal sustantivo, al derecho procesal y la cooperación internacional, en atención a la complejidad que caracteriza al cibercrimen.

Respecto a las medidas que deben adoptarse a nivel de **derecho penal sustantivo**, se exige que las partes adopten las medidas legislativas y de otro tipo, que resulten necesarias para tipificar como delito en su derecho interno, los delitos contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos que se establecen en el Capítulo II del Convenio, tales como: acceso ilícito, interceptación ilícita, ataques a la integridad de datos, ataques a la integridad del sistema y abuso de los dispositivos; delitos informáticos, como la falsificación informática y el fraude informático; delitos relacionados con la pornografía infantil; y delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines.

Respecto a las exigencias relativas al **derecho procesal**, las partes deben adoptar aquellas medidas legislativas y de otro tipo, que resulten necesarias para establecer los poderes y procedimientos presentes en la Sección 2 del Convenio, a los efectos de una investigación o procedimientos penales específicos, tales como: la preservación expeditiva de los datos informáticos almacenados, preservación expeditiva y divulgación parcial de los datos de tráfico, orden de presentación, búsqueda e incautación de datos informáticos, obtención en tiempo real de datos relativos al tráfico y la interceptación de datos de contenido.

Asimismo, en materia de **jurisdicción**, se exige que las partes adopten las medidas legislativas y de otro tipo, que resulten necesarias para afirmar su jurisdicción respecto de los delitos establecidos en el Convenio.

---

[1] **Natalia Molina Areal**, abogada (Universidad Católica de Santiago del Estero); Diplomada en Derecho Procesal Penal (Universidad Austral); Especialista en Derecho Penal (Universidad Nacional de Rosario) y Maestranda en Derecho Penal (Universidad Austral).

Finalmente, en materia de **cooperación internacional** se establecen principios generales relativos a la asistencia mutua en relación con los delitos tradicionales y con los delitos relacionados a la informática.

Da cuenta de la asistencia mutua tradicional en dos situaciones: cuando entre las partes no existen fundamentos jurídicos (tratados, leyes de reciprocidad, etc.) en cuyo caso corresponde aplicar sus disposiciones, y cuando existe dicha base, en cuyo caso los acuerdos existentes también se aplican a la asistencia que se concede en virtud del Convenio. La asistencia específica en materia de delitos informáticos o de delitos relacionados con la informática se aplica a ambas situaciones.

Por otro lado, se exige la creación de una **Red 24/7** como punto de contacto localizable las veinticuatro horas del día, siete días a la semana, con el fin de 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. Que esta asistencia comprenderá toda acción que facilite las medidas de asesoramiento técnico, conservación de datos, y obtención de pruebas, suministro de información de carácter jurídico y localización de sospechosos.

Asimismo, el Convenio contiene una disposición sobre un tipo específico de acceso transfronterizo a los datos informáticos almacenados que no requieren asistencia mutua (con consentimiento o disponibles al público).

Se regulan cuestiones relativas a la **extradición**, y se otorga a los Estados la posibilidad de formular **reservas**, solo respecto de las cláusulas expresamente autorizadas por el mismo.

---

[1] **Natalia Molina Areal**, abogada (Universidad Católica de Santiago del Estero); Diplomada en Derecho Procesal Penal (Universidad Austral); Especialista en Derecho Penal (Universidad Nacional de Rosario) y Maestranda en Derecho Penal (Universidad Austral).

En el caso de **Argentina**, se aprobó el Convenio sobre Ciberdelito en el año 2017, mediante la sanción de la **Ley N.º 27.411**, efectuando una serie de reservas, por considerar que algunas de sus disposiciones son incompatibles o no se ajustan a nuestro derecho interno.

La pregunta que aquí cabe formularnos es, ¿Argentina, ha dado cumplimiento a las exigencias del Convenio, en materia derecho penal sustantivo, derecho procesal y cooperación internacional? Cuestión que analizaré en el siguiente apartado.

---

3. EL CIBERCRIMEN Y LOS DELITOS INFORMÁTICOS EN ARGENTINA

A nivel de legislación comparada, podemos advertir que la combinación de la delincuencia con las posibilidades que brindan las nuevas tecnologías ha generado que muchos países optaran por la generación de nuevas figuras penales de acciones relacionadas a la informática.

En el caso particular de Argentina, en materia de derecho penal sustantivo, se sancionó la Ley N.º 26.388, el 4 de junio del año 2008, promulgada el 24 y publicada el 25 del mismo mes y año. Esta, no es una ley especial de delitos informáticos con figuras propias y específicas, sino que consiste en una modificación difuminada del Código Penal, es decir, la nueva ley modificó, sustituyó e incorporó figuras típicas a diversos artículos del Código Penal vigente, con el objeto de regular y penalizar las nuevas tecnologías como medios de comisión de delitos.

---

[1] **Natalia Molina Areal**, abogada (Universidad Católica de Santiago del Estero); Diplomada en Derecho Procesal Penal (Universidad Austral); Especialista en Derecho Penal (Universidad Nacional de Rosario) y Maestranda en Derecho Penal (Universidad Austral).

Introdujo modificaciones relativas al ofrecimiento y distribución de imágenes relacionadas con la pornografía infantil (artículo 128 C.P.N), violación de secretos y privacidad (artículos 153, 153 bis, 155, 157, 157 bis C.P.N), estafa y otras defraudaciones (artículo 173, inciso 16, C.P.N.), daño (artículos 183 y 184, C.P.N.), interrupción de comunicaciones (artículo 197 C.P.N.), destrucción de prueba (artículo 255 C.P.N.) y a su vez, incorporó al artículo 77 del C.P.N, definiciones conceptuales de los términos «documento», «firma», «suscripción», «instrumento privado» y «certificado», indispensables para permitir una interpretación precisa de los tipos penales, a la luz del principio de legalidad, respecto de la reforma producida en relación a la criminalidad informática como modo comisivo de los tipos penales recientemente enunciados.

Posteriormente, el 13 de noviembre del año 2013, se sancionó en nuestro país la Ley 26.904, publicada en el Boletín Oficial el 11 de diciembre del mismo año, mediante la cual se incorporó el artículo 131 al Código Penal, tipificando el delito de grooming.

Sin embargo, cabe preguntarnos, *¿resulta suficiente con la sanción de estas leyes, o todavía debemos avanzar un poco más para crear nuevos tipos penales, modificar o adaptar a las nuevas tecnologías, otros delitos ya existentes en el Código penal, pero que no fueron incluidos en las mismas*?

A mi humilde entender, si bien hemos dado un paso fundamental al tomar consciencia de esta problemática, al sancionar leyes en la materia, y adherirnos como Estado-parte al Convenio de Budapest, considero que dimos el paso inicial en la penalización de estos ilícitos, pero que *resta un largo camino que transitar*, porque no se han penalizado, todavía, ciertos comportamientos delictivos que se presentan con bastante frecuencia, y que son producto de las nuevas tecnologías.

---

[1] **Natalia Molina Areal**, abogada (Universidad Católica de Santiago del Estero); Diplomada en Derecho Procesal Penal (Universidad Austral); Especialista en Derecho Penal (Universidad Nacional de Rosario) y Maestranda en Derecho Penal (Universidad Austral).

Sin dejar de sopesar el problema que surge de la vertiginosa velocidad con la que estas últimas evolucionan, y el consiguiente cambio y desarrollo, también extremadamente rápido, de las conductas delictivas vinculadas a ellas.

A modo de ejemplo, puedo mencionar el llamado «revenge porn» o «porno venganza», que consiste en la difusión, sin el consentimiento de la víctima, de imágenes, videos o fotografías, que, si bien se han obtenido con su consentimiento, en un contexto de intimidad, no estaban destinadas a ser difundidas ni publicadas, y que, por lo general, son llevadas a cabo por exparejas o personas que buscan vengarse luego de una ruptura o pelea, siendo las mujeres las víctimas principales.

Esta conducta, que es llevada a cabo gracias al avance de la tecnología: Internet, mayormente redes sociales, servicio de mensajería instantánea o cualquier tipo de medio social donde se comparte información, a diferencia de otros países, **no se encuentra tipificada como delito específico en el Código Penal Argentino**.

Sin embargo, en la Ciudad Autónoma de Buenos Aires, se encuentra regulada como una «contravención», pero surge el interrogante de ¿qué sucede con aquellas provincias como, Santiago del Estero, que no reguló esta conducta ni siquiera como una contravención? La respuesta es que hoy, en mi provincia, la difusión de imágenes no consentida es una **conducta atípica e impune como tal**. Lo mismo sucede con la llamada «suplantación de identidad» o «sextorsión o extorsión sexual».

Yendo ahora al terreno del derecho procesal, cabe preguntarnos ¿es realmente necesario modificar o adaptar a las nuevas tecnologías, los códigos procesales penales de todas las provincias, cuando tenemos un principio de

---

[1] **Natalia Molina Areal**, abogada (Universidad Católica de Santiago del Estero); Diplomada en Derecho Procesal Penal (Universidad Austral); Especialista en Derecho Penal (Universidad Nacional de Rosario) y Maestranda en Derecho Penal (Universidad Austral).

libertad probatoria, que nos permite echar mano a medios de prueba que no están expresamente contemplados, para comprobar nuestra hipótesis o teoría del caso?

La doctrina mayoritaria considera que es necesaria su reforma para regular la evidencia informática o digital, debiéndose además incluir normativa que regule las telecomunicaciones y la cooperación internacional en materia penal. Máxime, si atendemos a la manifestación del crimen organizado y su proyección transnacional. Personalmente, comparto esta postura.

Aquí ingresamos al terreno de lo que sería la investigación de los delitos informáticos y la llamada evidencia digital. En términos generales, cuando hablamos de evidencia digital, nos referimos a todo registro informático almacenado en un dispositivo informático o que se transmite a través de una red informática, y que pudiera tener valor probatorio para una investigación. Entre las características que presenta la evidencia digital, podemos decir que la misma es volátil, ya que si no es preservada adecuadamente, puede cambiar o variar con facilidad de forma poco previsible; duplicable, ya que puede ser duplicada de manera exacta, y copiada tal como si fuese el original; alterable y modificable, con las herramientas adecuadas es relativamente fácil destruir, alterar o modificar; eliminable, ya que puede ser eliminada por completo utilizando las herramientas correctas.

Al comienzo de mi presentación me formulaba la siguiente pregunta: ¿en Argentina, estamos capacitados para enfrentarnos a estas nuevas modalidades delictivas?, y a ello le podemos agregar, ¿los Códigos Procesales Penales nos brindan las herramientas necesarias para investigar en entornos digitales?

Personalmente, considero que necesitamos adaptar los códigos procesales penales a estas nuevas modalidades de investigación y a las nuevas tecnologías,

---

[1] **Natalia Molina Areal**, abogada (Universidad Católica de Santiago del Estero); Diplomada en Derecho Procesal Penal (Universidad Austral); Especialista en Derecho Penal (Universidad Nacional de Rosario) y Maestranda en Derecho Penal (Universidad Austral).

e incorporar medidas de investigación específicas, ya que, cuando hablamos de recolección de evidencia digital o de investigación en entornos digitales, la cuestión se torna más compleja, y, claramente, no es lo mismo realizar una «investigación tradicional en espacios físicos» que realizar una «investigación en entornos digitales».

Los códigos procesales penales vigentes en Argentina, por lo general se refieren a «cosas, objetos, bienes o documentos», pero aquí estamos hablando de «datos», datos o información que se encuentra almacenada dentro de esa cosa u objeto, dentro de dispositivos, como ser una computadora, un teléfono celular, etc. por lo que necesitamos acceder al interior de ese dispositivo, navegar dentro del mismo, para buscar, por ejemplo, aquellos mensajes que formaron parte de una amenaza extorsiva, o el material de una explotación sexual infantil.

En el marco de una investigación de estas características, no solo debemos solicitarle al juez una orden de allanamiento para proceder al secuestro de la «cosa: computadora» (como lo haríamos en el ámbito de una investigación tradicional) sino que, además, le debemos pedir autorización para acceder a la misma, porque en este caso, yo no necesito la cosa en sí, sino los datos que la cosa almacena, los que luego serán objeto de una pericia. Ello demuestra que el panorama cambia, y entran en juego derechos constitucionales que debemos preservar, como ser, **el derecho a la intimidad o privacidad**, cuestión que abordaré más adelante.

Pero el «problema» no termina allí, porque puede suceder que los datos o la información que necesite, no se encuentre alojada en el disco local de la computadora secuestrada, sino que se encuentre almacenada en la nube, o en un servidor extranjero, o, que se encuentre, por ejemplo, en cuentas privadas de redes sociales que pertenecen a empresas como ser Facebook, Instagram o

---

[1] **Natalia Molina Areal**, abogada (Universidad Católica de Santiago del Estero); Diplomada en Derecho Procesal Penal (Universidad Austral); Especialista en Derecho Penal (Universidad Nacional de Rosario) y Maestranda en Derecho Penal (Universidad Austral).

Twitter, y con ello aparece en escena el sector privado como protagonista, y también aparece un gran enemigo: el tiempo.

Y es que el tiempo es un gran enemigo para la investigación en entornos digitales, porque estas empresas no tienen la obligación de guardar todos los datos de sus clientes, como tampoco tienen la obligación de responder a los requerimientos de la justicia (sin perjuicio de que en la mayoría de los casos responden), y puede suceder que cuando el fiscal a cargo de una investigación formule un requerimiento a la red social Facebook para que le proporcione cierta información relativa a determinada persona, haya pasado cierto tiempo y Facebook ya haya eliminado esa información y, como consecuencia, se frustra la investigación.

A modo de síntesis, podemos decir entonces, que la evidencia digital puede encontrarse almacenada en dispositivos informáticos (discos rígidos, por ejemplo); en la memoria RAM de procesamiento de un sistema informático; o bien, cuando se transmite a través de una red de dispositivos cuya recolección se realizará en tiempo real (tráfico de datos). En este contexto, el hardware está conformado por todos los componentes físicos de un sistema informático, mientras que la información se refiere a los datos, programas almacenados y mensajes de datos transmitidos usando el sistema informático.

Por otro lado, es necesario destacar que si bien, en el marco de una investigación, siempre trabajamos de manera interdisciplinaria, en este tipo de investigaciones es muy importante contar con personas especializadas, capacitadas en la recolección de evidencia digital, como, por ejemplo, con ingenieros informáticos, que sepan cómo extraer correctamente un dato informático, como almacenarlo para no dañarlo, etc. Y es necesario además que

---

[1] **Natalia Molina Areal**, abogada (Universidad Católica de Santiago del Estero); Diplomada en Derecho Procesal Penal (Universidad Austral); Especialista en Derecho Penal (Universidad Nacional de Rosario) y Maestranda en Derecho Penal (Universidad Austral).

cuenten con aquellas herramientas o medios técnicos adecuados, «sofisticados», que les permitan acceder a aquellos dispositivos.

Es por todo ello, que podemos advertir que la recolección de evidencia digital es muy compleja, y que su correcto tratamiento es fundamental para que sea admisible como prueba en un eventual juicio: debe haberse obtenido respetando las garantías y procedimientos legales, basada en una previa autorización judicial, justificando su tratamiento en los procedimientos de obtención, preservación, análisis y presentación ante el tribunal, respetando la cadena de custodia.

Como mencioné anteriormente, en una investigación en entornos digitales, al igual que en una investigación en entornos físicos, se deben respetar todas y cada una de las garantías constitucionales que les asisten a las personas sospechosas de cometer un delito. Sucede que, cuando comenzamos a navegar y analizar los dispositivos electrónicos secuestrados, nos encontramos con toda la vida de una persona, entonces, la pregunta es ¿hasta dónde podemos «navegar» sin vulnerar su derecho a la intimidad? ¿en dónde se encuentra el límite?

Aquí surge toda una discusión relacionada con la doctrina de la plain view: hasta qué punto podemos hablar de encuentros casuales cuando me encuentro con toda esa información a mi alcance, cuestión que excede el tema en análisis. Pero sí quiero remarcar que es muy importante tener en claro qué es lo que buscamos para comprobar nuestra teoría del caso a la hora de procesar y analizar la información.

Finalmente, en atención a los compromisos internacionales asumidos por Argentina, resta tratar la cuestión relativa a la exigencia de reforzar los mecanismos de cooperación internacional en la lucha contra el cibercrimen.

---

[1] **Natalia Molina Areal**, abogada (Universidad Católica de Santiago del Estero); Diplomada en Derecho Procesal Penal (Universidad Austral); Especialista en Derecho Penal (Universidad Nacional de Rosario) y Maestranda en Derecho Penal (Universidad Austral).

Como ha quedado demostrado, la cibercriminalidad se caracteriza, entre otras cosas, por su transnacionalidad, lo que pone a todos los Estados en una relación estrecha, y exige una cooperación eficaz para poder hacer frente a este fenómeno.

En cumplimiento del Convenio sobre Ciberdelito del cual somos parte, se ha dictado en nuestro país, la Resolución N.º 1291/2019 en el marco del Ministerio de Justicia y Derechos Humanos de la Nación, que creó la Unidad 24/7 con el objetivo de servir como un punto de contacto localizable, habiendo sido publicada el 27 de noviembre del año 2019 en el Boletín Oficial.

Que según surge de la mencionada resolución, dicha Unidad, funcionará en la órbita de la Dirección Nacional de Asuntos Internacionales, dependiente de la Unidad de Coordinación General del Ministerio de Justicia y de Derechos Humanos de la Nación, y actuará en forma coordinada con el Ministerio de Relaciones Exteriores y Culto como órgano central de cooperación internacional en materia penal y autoridad central designada en el marco del Convenio para la tramitación de solicitudes de asistencia mutua.

Asimismo, surge de la mencionada Resolución, que la Unidad 24/7 tiene como funciones, asegurar la asistencia inmediata en la investigación de infracciones penales llevadas a cabo a través de sistemas y datos informáticos, y en la recolección de pruebas electrónicas de una infracción penal. Esta asistencia comprende, en la medida permitida por la normativa aplicable, facilitar la aplicación directa de las siguientes medidas: a) aportación de consejos técnicos; b) conservación de datos según lo dispuesto en los artículos 29 y 30 del Convenio de Budapest; y, c) recolección de pruebas, aportación de información de carácter jurídico y localización de sospechosos.

---

[1] **Natalia Molina Areal**, abogada (Universidad Católica de Santiago del Estero); Diplomada en Derecho Procesal Penal (Universidad Austral); Especialista en Derecho Penal (Universidad Nacional de Rosario) y Maestranda en Derecho Penal (Universidad Austral).

A modo de síntesis, y habiéndose analizado, en términos generales, el cibercrimen y los delitos informáticos en Argentina, puedo concluir este acápite advirtiendo que, en materia de derecho penal sustantivo, nos falta legislar más, para tipificar como delitos en nuestro derecho interno, aquellas conductas delictivas relacionadas con la informática, que no encuentran una figura específica en el Código Penal; en materia de derecho procesal, considero que necesitamos reformar los códigos procesales penales, para incorporar técnicas de investigación o procedimientos penales específicos en la materia; y en lo que respecta a los mecanismos de cooperación internacional, deberíamos seguir trabajando para reforzarlos cada vez más, pero sobre todo hacia el interior del país, mediante su implementación y un eficaz funcionamiento a nivel provincial.

---

4. EL CIBERCRIMEN Y LA EVIDENCIA DIGITAL EN LA PROVINCIA DE SANTIAGO DEL ESTERO

En la provincia de Santiago del Estero, a diferencia de lo que ocurre por ejemplo, en la Ciudad Autónoma de Buenos Aires, no se creó una unidad fiscal especializada en materia de cibercrimen o delitos informáticos, sino que las denuncias formuladas por este tipo de delitos, serán competencia, según el caso y, según el bien jurídico protegido por la norma invocada, de los fiscales de las Unidades de Investigación y Litigación (por ejemplo, ante una denuncia por el delito de daño informático en virtud del art. 183 del C.P.N), o de las Unidades de Abuso Sexual (ante una denuncia por el delito de pornografía infantil, en virtud del art. 128 del C.P.N, o de grooming, tipificado en el art. 131 del C.P.N) o de las Unidades de Violencia de Género e Intrafamiliar, respecto de cualquier delito informático o cometido a través de Internet, en el marco de una relación de pareja o ex pareja.

---

[1] **Natalia Molina Areal**, abogada (Universidad Católica de Santiago del Estero); Diplomada en Derecho Procesal Penal (Universidad Austral); Especialista en Derecho Penal (Universidad Nacional de Rosario) y Maestranda en Derecho Penal (Universidad Austral).

Hace no mucho tiempo, existió en la provincia de Santiago del Estero, una denuncia penal «mediática», formulada por una persona de sexo femenino, que ostenta un cargo importante en la justicia santiagueña, en la que manifestaba que su ex pareja la amenazaba con publicar en las redes fotos en las que aparecía desnuda, que, en el caso de haberse consumado la difusión de dichas imágenes, configuraría un claro ejemplo de «revenge porn», actualmente impune tanto como delito y como contravención en la provincia.

En este caso, la denuncia fue derivada a la Unidad Fiscal de Violencia de Género e Intrafamiliar de turno, que fue la competente en razón de haber existido entre las partes una relación de pareja, decidiendo la fiscal interviniente, imputar al denunciado el delito de amenazas simples, en virtud del art. 149 Bis del Código Penal.

En materia de investigación en entornos digitales y recolección de evidencia digital, el Ministerio Público Fiscal de la provincia cuenta con el Gabinete de Ciencias Forenses, y dentro de la Policía de la provincia, se creó el Departamento de Ciberseguridad, ambos, encargados de la recolección de evidencia digital, con personal especializado en la materia.

Recuerdo un caso que me tocó investigar como instructora de la Unidad Fiscal de Violencia de Género e Intrafamiliar, en la que una persona de sexo femenino formuló una denuncia penal en contra de su ex pareja, quien estando privado de su libertad cumpliendo condena efectiva en el Servicio Penitenciario Federal de Colonia Pinto, le enviaba mensajes de texto, como así también audios vía WhatsApp, y le realizaba llamadas telefónicas para amenazarla de muerte por haber finalizado la relación.

---

[1] **Natalia Molina Areal**, abogada (Universidad Católica de Santiago del Estero); Diplomada en Derecho Procesal Penal (Universidad Austral); Especialista en Derecho Penal (Universidad Nacional de Rosario) y Maestranda en Derecho Penal (Universidad Austral).

Que de inmediato, la denunciante hizo entrega voluntaria de su teléfono celular para realizar la correspondiente investigación y extracción de evidencia. Por orden de la fiscal de la causa, se ofició al Gabinete de Ciencias Forenses del Ministerio Público Fiscal, solicitando la preservación de la evidencia digital mediante la extracción de datos del dispositivo móvil, como así también se ofició al Departamento de Ciberseguridad de la policía, a quienes se solicitó que investiguen sobre: titularidad y datos contractuales de las líneas implicadas, impactación histórica del IMEI, titularidad, llamadas entrantes y salientes de los números que impactaron en ese IMEI, con indicación de las celdas que intervinieron y sus direcciones, los mensajes de textos entrantes y salientes, las titularidades de las líneas que llamaron y mensajes en determinado periodo, informe de ubicación de impacto de antenas y/o torres, celda y micro celdas y azimut, especificando dirección exacta de antenas con nombre, calle, altura, barrio, ciudad, provincia y coordenadas, etc. solicitando se remita a la Unidad Fiscal interviniente, el informe correspondiente para su posterior análisis.

En cumplimiento de la intervención solicitada, el Departamento de Ciberseguridad se contactó con las empresas de WhatsApp y Telecom Personal, quienes remitieron sus respectivos informes y, con ellos, se pudo comprobar que efectivamente los mensajes y llamadas telefónicas provenían de la zona donde el denunciado se encontraba privado de su libertad, como así también se obtuvo el registro de las llamadas, con indicación de número, fecha, nombre, DNI, dirección, ciudad, provincia, y, el contenido de las mismas, se pudo constatar a través del análisis de los datos extraídos del celular de la víctima.

Este es un ejemplo de un «delito tradicional»: amenazas, cometido mediante el uso de la tecnología, en el que fue necesario recurrir a la recolección y análisis de evidencia digital, ya que la prueba del delito se encontraba alojada en el interior del dispositivo móvil de la denunciante.

---

[1] **Natalia Molina Areal**, abogada (Universidad Católica de Santiago del Estero); Diplomada en Derecho Procesal Penal (Universidad Austral); Especialista en Derecho Penal (Universidad Nacional de Rosario) y Maestranda en Derecho Penal (Universidad Austral).

Ahora, ¿qué sucede con el Código Procesal Penal de la Provincia de Santiago del Estero? si bien el mismo fue modificado por última vez el 17 de marzo del año 2009, no se incorporaron procedimientos específicos relativos a la recolección de evidencia digital, por lo que en mi opinión, resulta necesaria una próxima modificación para su pronta regulación.

---

5. CIBERPATRULLAJE

En materia de prevención y/o investigación de ciberdelitos, es importante mencionar lo que se conoce como ciberpatrullaje.

Según enseña la Dra. Daniela Dupuy, Fiscal de Delitos Informáticos de la Ciudad Autónoma de Buenos Aires, debemos distinguir, el ciberpatrullaje realizado en el marco de una investigación penal concreta, del ciberpatrullaje realizado por las fuerzas de seguridad de un Estado de manera indiscriminada.

La técnica del ciberpatrullaje se encuentra aceptada y recepcionada por la jurisprudencia a nivel internacional, siempre y cuando se realice correctamente, es decir, en el marco de una investigación penal concreta en entornos digitales y respetando las garantías constitucionales: el límite está marcado por el derecho a la intimidad o privacidad de la persona que se investiga.

Cambió la modalidad de cometer delitos y cambió la manera de investigar. De hecho, en todas las fiscalías modernas de cibercrimen del mundo, se utilizan las llamadas *técnicas de investigación en fuentes abiertas*, que consisten en procesar información pública, es decir, aquella información que nosotros mismos, como usuarios, colocamos en las redes sociales. No se trata de información que se

---

[1] **Natalia Molina Areal**, abogada (Universidad Católica de Santiago del Estero); Diplomada en Derecho Procesal Penal (Universidad Austral); Especialista en Derecho Penal (Universidad Nacional de Rosario) y Maestranda en Derecho Penal (Universidad Austral).

obtiene mediante la intromisión indebida al perfil privado del usuario, sino de información pública.

No obstante, si debemos traspasar ese límite e inmiscuirnos en una *fuente privada*, el panorama cambia, y es necesario solicitar al juez la correspondiente autorización, so pena de incurrir en una nulidad que nos haga caer todo el procedimiento por vulneración del derecho a la intimidad.

Distintas son las tareas de ciberpatrullaje o ciberespionaje realizadas por miembros de las fuerzas de seguridad con fines de inteligencia, en las que se monitorean de forma masiva e indiscriminada las redes sociales, con la supuesta finalidad de «anticiparse a la comisión de delitos».

Tales prácticas, que consisten en observar lo que las personas publican, sin definir previamente qué se busca, a quienes, ni por qué se observa, son conocidas como «excursiones de pesca» y están estrictamente prohibidas por leyes locales e internacionales, ya que no cumplen salvaguardas básicas de derechos humanos, tales como la legalidad, la necesidad y la proporcionalidad, afectando al mismo tiempo, la privacidad y libertad de expresión de las personas.

En Argentina, como en otros lugares del mundo, solo los servicios de inteligencia nacional están facultados por la ley para realizar actividades de inteligencia nacional, con límites estrictos. De hecho, en nuestro país se sancionó la Ley 25.520, modificada por la ley 27.126, de donde surge que «se entenderá por inteligencia nacional, a la actividad consistente en la obtención, reunión, sistematización y análisis de la información específica referida a los hechos, riesgos y conflictos que afecten la Defensa Nacional y la seguridad interior de la Nación», disponiendo que el funcionamiento del Sistema de Inteligencia Nacional deberá ajustarse estrictamente a las previsiones contenidas en la

---

[1] **Natalia Molina Areal**, abogada (Universidad Católica de Santiago del Estero); Diplomada en Derecho Procesal Penal (Universidad Austral); Especialista en Derecho Penal (Universidad Nacional de Rosario) y Maestranda en Derecho Penal (Universidad Austral).

Constitución Nacional, en las normas legales y reglamentarias vigentes, y que ningún organismo de inteligencia podrá cumplir, por sí, funciones policiales, como así tampoco, funciones de investigación criminal, salvo ante requerimiento específico y fundado realizado por autoridad judicial competente en el marco de una causa concreta sometida a su jurisdicción, o que se encuentre, para ello, autorizado por ley, en cuyo caso le serán aplicables las reglas procesales correspondientes.

En este punto, estaríamos ingresando a un terreno de análisis muy interesante pero que excede el propósito de este trabajo, por lo que concluiré este acápite diciendo que las actividades de inteligencia masiva e indiscriminada están prohibidas, y que el ciberpatrullaje solo se encuentra permitido cuando es realizado dentro de los límites legales y constitucionales.

CONCLUSIONES

Las estadísticas indican que las actividades informáticas delictivas están en crecimiento a nivel global. El ingreso de los casos de delitos informáticos o cometidos a través de las nuevas tecnologías, o de Internet, a las fiscalías penales, se encuentra en constante aumento, principalmente desde la aparición de la pandemia por Covid-19.

Las estadísticas actuales demuestran que la web es uno de los medios más elegidos por los autores o partícipes de ciertos delitos, como, por ejemplo, de pornografía infantil, ya que existe un problema de identificación de los autores con base en el teórico anonimato que proporciona la red.

---

[1] **Natalia Molina Areal**, abogada (Universidad Católica de Santiago del Estero); Diplomada en Derecho Procesal Penal (Universidad Austral); Especialista en Derecho Penal (Universidad Nacional de Rosario) y Maestranda en Derecho Penal (Universidad Austral).

Uno de los problemas esenciales consiste en determinar quién o quiénes son responsables jurídico-penalmente de entre todos los intervinientes, ya que existen organizaciones internacionales, dispersas por todo el mundo, con una organización sofisticada y que saben «manipular» los sistemas.

Por otro lado, ante un fenómeno tan complejo, resulta fundamental la capacitación y el entrenamiento constante de los investigadores, técnicos y fiscales para un correcto procedimiento, exento de falencias u objeciones procesales.

Desde mi punto de vista, en Argentina necesitamos legislar más en materia de delitos informáticos, no solo a nivel legislación de fondo, tipificando aquellas conductas que todavía no constituyen delitos, sino también a nivel de legislación de forma.

Los códigos procesales penales demandan una modificación, de modo que permitan investigar correctamente en entornos digitales, no solo desde el punto de vista del Estado que investiga, sino también desde el punto de vista de las garantías y los derechos que les asisten a las personas investigadas.

En la práctica diaria surgen claras dificultades relacionadas con la evidencia digital, nueva protagonista de los delitos cometidos a través medios digitales, absolutamente diferente a la evidencia física, e implica la adopción de métodos específicos para su recolección y preservación.

Por otro lado, considero que debemos reforzar los mecanismos de cooperación internacional, recordando que la información y la comunicación fluyen con mayor facilidad por todo el mundo y que las fronteras han dejado de ser barreras para ese flujo.

---

[1] **Natalia Molina Areal**, abogada (Universidad Católica de Santiago del Estero); Diplomada en Derecho Procesal Penal (Universidad Austral); Especialista en Derecho Penal (Universidad Nacional de Rosario) y Maestranda en Derecho Penal (Universidad Austral).

Los delincuentes se encuentran cada vez menos en los lugares en que se hacen sentir los efectos de sus actos y la legislación nacional está confinada generalmente a un territorio específico. Es por ello, que las soluciones a muchos de los problemas planteados deben ser abordadas por el derecho internacional, lo que requiere la adopción de instrumentos jurídicos internacionales adecuados, e invertir en tecnología sofisticada que nos permita una correcta investigación para poder acceder a información de difícil acceso.

La investigación del cibercrimen y los delitos informáticos constituye uno de los desafíos más complejos para los sistemas de justicia contemporáneos, particularmente en países como Argentina donde persisten vacíos normativos, limitaciones de recursos y asimetrías regionales significativas.

El análisis efectuado permite arribar a tres conclusiones fundamentales: en primer lugar, resulta impostergable la reforma legislativa tanto en el plano sustantivo como procesal. La existencia de conductas delictivas no tipificadas —como el revenge porn, la suplantación de identidad digital o la sextorsión específica— genera zonas de impunidad que los ciberdelincuentes aprovechan sistemáticamente. Los códigos procesales penales vigentes, diseñados para evidencia física y territorial, resultan inadecuados para regular la obtención, preservación y análisis de evidencia digital que fluye sin fronteras y presenta características radicalmente diferentes: volatilidad, duplicabilidad y desterritorialización.

En segundo término, la capacitación y especialización de los operadores jurídicos emerge como condición *sine qua non* para una persecución penal eficaz. La complejidad técnica de estos ilícitos demanda no solo conocimientos jurídicos sino también competencias en informática forense, análisis de metadatos,

---

[1] **Natalia Molina Areal**, abogada (Universidad Católica de Santiago del Estero); Diplomada en Derecho Procesal Penal (Universidad Austral); Especialista en Derecho Penal (Universidad Nacional de Rosario) y Maestranda en Derecho Penal (Universidad Austral).

técnicas de investigación en fuentes abiertas y comprensión de arquitecturas de redes.

La creación de unidades fiscales especializadas —como las existentes en Ciudad Autónoma de Buenos Aires pero ausentes en provincias como Santiago del Estero— constituye un modelo a replicar, acompañado de inversión sostenida en laboratorios de ciberforense y herramientas tecnológicas adecuadas.

Finalmente, la naturaleza transnacional del cibercrimen torna indispensable el fortalecimiento de los mecanismos de cooperación internacional. Si bien la adhesión argentina al Convenio de Budapest y la creación de la Unidad 24/7 representan avances significativos, su implementación efectiva requiere no solo marcos normativos sino también protocolos ágiles, personal especializado disponible y canales de comunicación fluidos con prestadores de servicios de Internet y autoridades extranjeras. La asimetría entre la velocidad del delito —que se ejecuta en fracciones de segundo— y la lentitud de los procedimientos de asistencia jurídica internacional, constituye una ventana de oportunidad que la criminalidad organizada explota sistemáticamente.

El cibercrimen no es un fenómeno futuro sino una realidad presente que exige respuestas inmediatas. Argentina cuenta con recursos humanos calificados, experiencia jurisdiccional acumulada y adhesión a instrumentos internacionales relevantes. Lo que resta es voluntad política para traducir esos recursos en reformas legislativas concretas, inversión presupuestaria sostenida y políticas públicas coordinadas entre el Estado nacional y las provincias. La alternativa es resignarnos a una impunidad creciente que erosiona la confianza ciudadana en el sistema de justicia y perpetúa la victimización en el espacio digital, donde cada vez más argentinos desarrollan su vida personal, profesional y económica. El tiempo de la acción es ahora.

---

[1] **Natalia Molina Areal**, abogada (Universidad Católica de Santiago del Estero); Diplomada en Derecho Procesal Penal (Universidad Austral); Especialista en Derecho Penal (Universidad Nacional de Rosario) y Maestranda en Derecho Penal (Universidad Austral).

Debemos preocuparnos por estas nuevas modalidades delictivas, pero también **ocuparnos**, y creo, que, como país, tenemos los recursos que se necesitan para invertir en la lucha contra la ciberdelincuencia.

BIBLIOGRAFÍA

Consejo de Europa (2001). Convenio sobre Ciberdelito. Budapest, Hungría. Recuperado de https://www.coe.int

Fillia, L. C., Sueiro, C. C., Monteleone, R., Nager, H. S., & Rosende, E. E. Análisis de la reforma en materia de cibercriminalidad informática al Código Penal de la Nación (ley 26.388).

Ley Nacional N.º 25.520 (2001). Ley de Inteligencia Nacional. Modificada por Ley N.º 27.126. Buenos Aires: Boletín Oficial de la República Argentina.

Ley Nacional N.º 26.388 (2008). Modificación del Código Penal. Delitos Informáticos. Buenos Aires: Boletín Oficial de la República Argentina.

Ley Nacional N.º 26.904 (2013). Modificación del Código Penal. Grooming. Buenos Aires: Boletín Oficial de la República Argentina.

Ley Nacional N.º 27.411 (2017). Aprobación del Convenio sobre Ciberdelito. Buenos Aires: Boletín Oficial de la República Argentina.

Ministerio de Justicia y Derechos Humanos de la Nación Argentina. Ciberdelitos. Recuperado de https://www.argentina.gob.ar

---

[1] **Natalia Molina Areal**, abogada (Universidad Católica de Santiago del Estero); Diplomada en Derecho Procesal Penal (Universidad Austral); Especialista en Derecho Penal (Universidad Nacional de Rosario) y Maestranda en Derecho Penal (Universidad Austral).

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.

Nessi, A. M. Manual de Evidencia Digital.

Pisanu, G. Ciberpatrullaje en Argentina: los riesgos del monitoreo de redes sociales para los derechos humanos. Access Now. Recuperado de www.accessnow.org

Resolución PGN N.º 1291/2019 (2019). Creación de la Unidad 24/7. Ministerio de Justicia y Derechos Humanos de la Nación. Buenos Aires: Boletín Oficial de la República Argentina.

Temperini, M. Delitos informáticos y cibercrimen: alcance, concepto y características.

---

[1] **Natalia Molina Areal**, abogada (Universidad Católica de Santiago del Estero); Diplomada en Derecho Procesal Penal (Universidad Austral); Especialista en Derecho Penal (Universidad Nacional de Rosario) y Maestranda en Derecho Penal (Universidad Austral).