LA EVIDENCIA DIGITAL EN LA LUCHA CONTRA EL CIBER-CRIMEN: DESAFÍOS EN SU OBTENCIÓN, PRESERVACIÓN Y USO EN ARGENTINA

(DIGITAL EVIDENCE IN THE FIGHT AGAINST CYBERCRIME: CHALLENGES IN ITS COLLECTION, PRESERVATION, AND USE IN ARGENTINA.)

Maximiliano Bendinelli[1]

RESUMEN

El presente trabajo examina los desafíos contemporáneos en la obtención, preservación y uso de evidencia digital en la lucha contra el cibercrimen en Argentina. Se analiza la evolución del panorama forense digital, destacando la implementación de protocolos estandarizados para mejorar el manejo de evidencias. El estudio aborda la creciente complejidad del cibercrimen, incluyendo nuevas modalidades delictivas facilitadas por las tecnologías de la información y comunicación.

Se exploran los retos técnicos y legales que enfrentan los investigadores, como el manejo de volúmenes masivos de datos, las amenazas a la seguridad informática, y la necesidad de cooperación internacional en la persecución de delitos transnacionales. El artículo destaca la importancia de herramientas forenses innovadoras y la capacitación continua de los operadores judiciales.

Se discuten los desafíos legales del allanamiento remoto, una técnica emergente que plantea interrogantes sobre privacidad y constitucionalidad. El estudio compara la situación de Argentina con estándares internacionales, identificando avances y áreas de mejora en la lucha contra el cibercrimen.

El artículo concluye enfatizando la necesidad de un enfoque multidisciplinario y una mayor cooperación internacional para enfrentar eficazmente las sofisticadas redes criminales en línea, adaptando constantemente los marcos legales y técnicos a la rápida evolución tecnológica.

PALABRAS CLAVE: *cibercrimen, evidencia digital, análisis forense digital, allanamiento remoto, seguridad informática, cooperación internacional.*

[1]*Magister en Seguridad Informática, Ingeniero en sistemas informáticos, Perito Informático del Cuerpo de Peritos del Poder Judicial de la Nación Especializados en Casos de Corrupción y Delitos contra la Administración Pública.*

Contacto: mbendinelli@csjn.gov.ar

ABSTRACT

This paper examines contemporary challenges in collecting, preserving, and using digital evidence in the fight against cybercrime in Argentina. It analyzes the evolution of the digital forensic outlook, highlighting the implementation of standardized protocols to improve evidence management. The study addresses the growing complexity of cybercrime, including new criminal modalities facilitated by information and communication technologies.

It explores the technical and legal challenges investigators face, such as the handling of massive volumes of data, threats to computer security, and the need for international cooperation in prosecuting transnational crimes. The article highlights the importance of innovative forensic tools and the continuous training of judicial operators.

This article discusses the legal challenges of remote forensics, an emerging technique that raises questions on privacy and constitutionality. The study compares the fight against cybercrime in Argentina with international standards, identifying progress and areas for improvement.

The article concludes by emphasizing the need for a multidisciplinary approach and greater international cooperation to effectively confront sophisticated online criminal networks, constantly adapting legal and technical frameworks to the rapid technological development.

KEYWORDS: *cybercrime, digital evidence, digital forensics, remote forensics, computer security, international cooperation, legislation and technology.*

Maximiliano Bendinelli[1]

[1]Magister en Seguridad Informática, Ingeniero en sistemas informáticos, Perito Informático del Cuerpo de Peritos del Poder Judicial de la Nación Especializados en Casos de Corrupción y Delitos contra la Administración Pública.

Contacto: mbendinelli@csjn.gov.ar

INTRODUCCIÓN

La evidencia digital se ha convertido en un elemento clave en la resolución de casos legales en las últimas décadas. Desde correos electrónicos hasta publicaciones en redes sociales, la información almacenada en dispositivos electrónicos puede proporcionar pruebas irrefutables de actividades ilegales o controvertidas y brindar pistas cruciales para esclarecer delitos.

Sin embargo, los rápidos avances tecnológicos también representan nuevos desafíos para los investigadores forenses en la recolección, análisis y presentación de este tipo de evidencia ante los tribunales. Asimismo, el uso masivo de redes de datos, Internet, redes sociales y cripto activos ha abierto nuevas modalidades de crimen transnacional que requieren respuestas coordinadas.

En Argentina, la situación del uso de evidencia digital en el ámbito forense ha experimentado una transformación significativa en los últimos años. Anteriormente, la falta de marcos legales específicos, la carencia de estándares técnicos uniformes y la escasa capacitación del personal policial y judicial en la manipulación y análisis de la evidencia digital generaban una serie de obstáculos para la investigación de delitos relacionados con las tecnologías de la información y la comunicación (TIC). La falta de un protocolo estandarizado conllevaba una alta posibilidad de contaminación o pérdida de la evidencia, y la admisibilidad de ésta en los tribunales se tornaba un proceso complejo e incierto.

Para afrontar estos desafíos, se han implementado una serie de protocolos, como el "Protocolo General de Actuación para las Fuerzas Policiales y de Seguridad en la Investigación y Proceso de Recolección de Pruebas en Ciberdelitos" (Resolución 234/2016)[1] y el "Protocolo de Actuación para la Investigación Científica en el Lugar del Hecho" (Resolución 528/2021)[2], que han ido mejorando gradualmente el panorama forense argentino.

El último avance en este sentido es la implementación del "Protocolo para la identificación, recolección, preservación, procesamiento y presentación de evidencia digital“, del Ministerio de Seguridad de la Nación, creado en el año 2023, bajo la Resolución 232/2023[3].Este protocolo, al igual que sus predecesores, busca estandarizar las prácticas y procedimientos para el manejo de la evidencia digital, asegurando su integridad, validez y admisibilidad en los tribunales.

Este artículo analiza algunos de los principales cambios y retos asociados al uso de evidencia digital en la actualidad, los desafíos que presenta su recolección y el impacto que ha tenido en el panorama legal moderno, tanto en la investigación de ciberdelitos como de otros ilícitos donde la informática es relevante, con un enfoque particular en la situación Argentina. Se exploran temas como la creciente cantidad de datos generados, las amenazas a la seguridad informática en la custodia de evidencias, las innovadoras herramientas y técnicas forenses disponibles, y los desafíos legales y de cooperación internacional que enfrentan los fiscales e investigadores en esta materia.

EXPLOSIÓN EN LA GENERACIÓN DE DATOS DIGITALES

Uno de los mayores desafíos que enfrentan los investigadores forenses es la enorme proliferación de datos digitales que deben recolectar y analizar en búsqueda de evidencias. Solo Facebook registró 2600 millones de usuarios activos

mensuales en 2018. Se estima que para 2025 se generarán globalmente 163 zettabytes de datos anuales[4].

Esta avalancha de información representa una invaluable fuente de pruebas potenciales para resolver crímenes. Pero también conlleva una tarea titánica en términos de tiempo y recursos necesarios para examinar volúmenes masivos de datos en dispositivos y aplicaciones *online*. Resulta en extremo difícil para los investígadores mantenerse al ritmo de la expansión exponencial de información digital relevante para la investigación de los casos.

NUEVAS AMENAZAS A LA SEGURIDAD INFORMÁTICA

Otro área que ha evolucionado drásticamente son las amenazas a la seguridad de la información que ponen en riesgo tanto a los investigadores forenses como a la integridad de la evidencia digital recolectada. Los ciberataques diseñados para borrar o alterar evidencias representan un grave peligro para el proceso investigativo y la cadena de custodia.

Los delincuentes informáticos se vuelven más sofisticados cada día, forzando a las fuerzas de la ley a dedicar cuantiosos recursos sólo para proteger sus propias operaciones forenses y los sistemas donde almacenan evidencia sensible. Se volvió indispensable tener robustos controles de seguridad para garantizar la autenticidad e inalterabilidad de la información digital obtenida, aspectos centrales para su valor probatorio. También hay que tener en cuenta los recursos que deben dedicar los estados para garantizar el acceso a herramientas y capacitaciones continuas, que ayuden a los investigadores a analizar los medios de prueba digitales y obtener resultados que permitan a los operadores judiciales resolver los casos sometidos a su conocimiento.

NUEVAS MODALIDADES DELICTIVAS CON LAS TICS

La expansión de Internet ha abierto nuevas modalidades de crimen transnacional, desafiando los esquemas tradicionales de investigación criminal.

Delitos como fraudes financieros, espionaje, robo de propiedad intelectual y difusión de material ilícito ahora trascienden fronteras con enorme facilidad. Las evidencias digitales relevantes para investigar estos ciberdelitos pueden hallarse dispersas en múltiples jurisdicciones. En Argentina, los fraudes financieros están tipificados en el Código Penal, específicamente en los artículos 173 y 174, que tratan sobre la estafa y la defraudación. El espionaje está contemplado en el artículo 157 bis del Código Penal. El robo de propiedad intelectual puede ser abordado bajo la Ley de Propiedad Intelectual (Ley 11.723) y la Ley de Marcas (Ley 22.362). La difusión de material ilícito, como la pornografía infantil, está tipificada en los artículos 128 y 129 del Código Penal.

Obtener tales evidencias de manera válida y efectiva requiere de una mayor coordinación y asistencia legal mutua entre países. También implica armonizar los marcos legales nacionales que regulan la recolección y admisibilidad de evidencia digital.

Algunas modalidades criminales han tomado nueva dimensión gracias a Internet y la adopción de la tecnología por individuos, empresas y gobiernos. Algunos de los delitos que a la fecha podríamos enumerar son la distribución de imágenes de abuso infantil, el ciberterrorismo para reclutamiento y propaganda, estafas masivas mediante *phishing*, y ataques contra infraestructura crítica de países y el secuestro de información a cambio de criptomonedas (*ransomware*).

Investigar estos complejos cibercrímenes de forma aislada resulta casi imposible. Se necesitan nuevos mecanismos de cooperación sistemática entre fuerzas policiales, fiscalías y judiciales a nivel global. Internet ha permitido la proliferación de verdaderas organizaciones criminales transnacionales que operan online.
Las técnicas de investigación también deben evolucionar, por ejemplo, mediante sofisticados operativos encubiertos en entornos digitales para infiltrar estas organizaciones. La evidencia forense digital es un elemento crítico en desbaratar su accionar, pero recolectarla representa un enorme reto, dada la naturaleza esquiva de estas redes delictivas.

¿CUÁL ES EL FUTURO DE LA EVIDENCIA DIGITAL EN EL MUNDO LEGAL?

La evidencia digital se ha vuelto omnipresente en los tribunales modernos, pero este área legal tan crucial se encuentra en un estado de rápida evolución tecnológica. ¿Qué depara el futuro para la recolección, análisis y uso de pruebas digitales?

Creciente volumen de datos
Con los antecedentes que existen, sería razonable esperar que la cantidad de información digital generada continúe expandiéndose de manera exponencial. Esto presentará desafíos sin precedentes de almacenamiento y procesamiento para los investigadores y operadores judiciales.

Nuevas tecnologías
Tecnologías como *blockchain* (cadenas de bloques) computación cuántica e inteligencia artificial transformarán la ciencia forense digital. Desde la detección de manipulación hasta el análisis de tendencias, las máquinas ayudarán a manejar e interpretar grandes conjuntos de datos.

Regulaciones cambiantes
A medida que evolucionan las tecnologías, también lo hacen las expectativas sociales de privacidad y los marcos legales. Los expertos forenses deberán mantenerse al día con las normas regulatorias en constante cambio.

Especialización creciente
La creciente complejidad de la evidencia digital requerirá mayor especialización.
Surgirán nuevas certificaciones y áreas de experiencia forense como la recuperación de datos móviles o *blockchain*.

HERRAMIENTAS INNOVADORAS Y TÉCNICAS FORENSES

Para afrontar estos obstáculos, los investigadores cuentan hoy con herramientas innovadoras y técnicas no disponibles hace apenas unos años. El análisis forense de elementos digitales puede revelar si un dispositivo fue hackeado y utilizado para actividades delictivas, sin consentimiento de su dueño. También existe un gran avance en recuperación de datos que ayudan a restaurar información incluso de unidades de almacenamiento muy dañadas; sin embargo el uso de nuevas tecnologías, como ser la utilización de discos de estado sólido, cambian el paradigma para la recuperación de datos eliminados.
Por otro lado, la computación en la nube está transformando los enfoques de recolección de evidencia al requerir nuevas técnicas para preservar datos en servidores remotos. Al mismo tiempo, ofrece eficientes opciones de procesamiento y almacenamiento para examinar enormes conjuntos de datos.
Tecnologías como inteligencia artificial, *machine learning* y *blockchains* empiezan a integrarse a los flujos de trabajo forenses. Se desarrollan nuevas herramientas específicamente diseñadas para decodificar y analizar evidencia digital multimedia. Mantenerse actualizado requiere una constante capacitación e inversión en infraestructura por parte de los organismos investigadores.

EL ALLANAMIENTO REMOTO

El allanamiento remoto es una "nueva" herramienta legal que permite a las autoridades acceder a dispositivos digitales sin necesidad de estar físicamente presentes en el lugar. Esta técnica plantea importantes cambios y desafíos en el ámbito de la evidencia forense digital y el cibercrimen.

Uno de los principales cambios es que facilita enormemente la recolección de evidencia digital por parte de los investigadores. Anteriormente estos debían presentarse físicamente en el lugar para incautar computadoras y dispositivos. Ahora, con una orden judicial, pueden acceder remotamente a esta información sin moverse de su oficina. Esto agiliza las investigaciones y permite recolectar evidencia que de otra forma sería más difícil o imposible de obtener.

Sin embargo, también introduce serios desafíos técnicos y legales. Desde el punto de vista técnico, realizar un allanamiento remoto requiere herramientas y conocimientos especializados para poder ingresar a los sistemas informáticos sin ser detectados y preservar la integridad de la evidencia. Los investigadores deben estar altamente capacitados en informática forense para llevar a cabo este tipo de procedimientos.

Sin embargo, el allanamiento remoto también plantea una serie de desafíos para la evidencia forense digital. En primer lugar, puede ser difícil garantizar la integridad de la evidencia recopilada. En segundo lugar, puede violar la privacidad de los usuarios. Por último, podría ser utilizado por los gobiernos para reprimir la libertad de expresión.

A nivel legal, se plantean dudas sobre la constitucionalidad y los límites de este tipo de allanamientos. ¿Hasta dónde puede llegar la intrusión del Estado en dispositivos digitales privados? ¿Se pone en riesgo el derecho a la intimidad y privacidad? Resolver estos interrogantes requerirá discusiones profundas y matizadas entre juristas, técnicos y sociedad civil. Otro cambio importante es la ubicuidad de los dispositivos digitales y la información que contienen. Teléfonos, computadoras y el "internet de las cosas" generan un flujo constante de datos que puede ser de interés en investigaciones penales. Esto expande enormemente el volumen y variedad de evidencia forense digital disponible.

Para las fuerzas de seguridad y agentes judiciales, esto representa un desafío mayúsculo en términos de procesamiento y análisis de datos. Se requieren nuevas plataformas informáticas, algoritmos de búsqueda e importantes capacidades de computación en la nube para extraer información útil para las investigaciones.

Asimismo, en el ámbito del cibercrimen, permite tanto a delincuentes como a las autoridades tener un amplio campo de acción. Los criminales cuentan con más superficie de ataque y vectores para cometer fraudes informáticos, distribuir programas malignos (malware) o acceder a información confidencial.

Pero los investigadores también tienen mucho más terreno para desplegar técnicas como la vigilancia de redes, el rastreo de actividad sospechosa en internet y la infiltración remota en equipos comprometidos. La batalla contra el cibercrimen se intensifica y globaliza.

DESAFÍOS LEGALES

El allanamiento remoto, como ya se mencionó, implica la posibilidad de acceder a información almacenada en dispositivos digitales sin la necesidad de una presencia física en el lugar. Esta técnica, si bien puede acelerar las investigaciones y permitir obtener pruebas que de otra forma serían inaccesibles, conlleva una serie de riesgos a la privacidad y a los derechos fundamentales de los individuos.

La Constitución de la Nación Argentina, en su artículo 19, protege el derecho a la

intimidad y a la privacidad. El allanamiento remoto, al permitir el acceso a información personal almacenada en dispositivos digitales, representa una injerencia en el ámbito privado del individuo que debe ser justificada con rigor y precisión.

Otro elemento crucial en el análisis legal del allanamiento remoto es el principio de reserva. Este principio exige una orden judicial para el acceso a la información personal. Su aplicación al allanamiento remoto requiere la definición de requisitos específicos que garanticen que la medida se aplica con la debida autorización judicial y que se respetan las garantías legales.

La jurisprudencia argentina aún no ha tenido la oportunidad de pronunciarse sobre la constitucionalidad del allanamiento remoto, lo que genera un vacío legal que debería ser subsanado. Un análisis profundo de la jurisprudencia existente sobre la interpretación del derecho a la intimidad, el principio de reserva y la aplicación de la prueba digital es crucial para determinar si la técnica del allanamiento remoto es compatible con el ordenamiento jurídico argentino.

La falta de un marco normativo específico para el allanamiento remoto genera una serie de desafíos procesales y de garantías. Se requiere un análisis profundo de los requisitos para la emisión de una orden judicial de allanamiento remoto. Deben definirse criterios específicos que garanticen la proporcionalidad de la medida y que se justifique la necesidad de acceder a la información de manera remota, en lugar de una intervención física. Es necesario establecer mecanismos de control judicial que aseguren que las órdenes de allanamiento remoto se emitan con las debidas garantías legales y que se respeten los derechos del investigado. Asimismo, se deben establecer mecanismos que aseguren la notificación oportuna al investigado, de manera que pueda ejercer sus derechos y proteger sus intereses. La cadena de custodia de la evidencia digital es fundamental para garantizar su admisibilidad en juicio. En el contexto del allanamiento remoto, se deben implementar procedimientos específicos para asegurar la integridad y autenticidad de la información obtenida.

DESAFÍOS PARA LA INTEGRIDAD DE LA EVIDENCIA

Uno de los principales desafíos del allanamiento remoto es garantizar la integridad de la evidencia recopilada. Cuando las fuerzas de seguridad acceden físicamente a un dispositivo informático, pueden tomar medidas para garantizar que la evidencia no se modifique, como crear una imagen forense del dispositivo. Sin embargo, cuando el allanamiento se realiza de forma remota, es más difícil garantizar que la evidencia no se altere ya que no existiría un contralor que convalide las actividades realizadas.

Las fuerzas de la ley pueden utilizar una variedad de técnicas para garantizar la integridad de la evidencia recopilada durante un allanamiento remoto. Por ejemplo, pueden utilizar un *software* de cifrado para proteger la evidencia durante la transmisión. También pueden utilizar un protocolo de auditoría para rastrear los cambios realizados en la evidencia. Por otro lado ¿quién garantiza la privacidad de los investigados?

DESAFÍOS LEGALES Y DE PRIVACIDAD

El uso de evidencia digital también plantea complejos desafíos legales y de privacidad. La legislación argentina al día de hoy no contempla los contextos tecnológicos actuales de manera adecuada. Si bien desde la creación del "Protocolo para la identificación, recolección, preservación, procesamiento y presentación de evidencia digital" del Ministerio de Seguridad de la Nación, se

definieron algunas pautas para la recolección de evidencia digital , no se definió el caso en el cual la adquisición de la evidencia sea remota sin darle conocimiento a la defensa , y por lo tanto, no está claro cómo aplicar las normas existentes para equilibrar los amplios poderes investigativos con la protección de derechos individuales.

Con la información personal que contienen los dispositivos y cuentas *online*, surgen serias preocupaciones respecto a la privacidad. Los investigadores forenses deben sopesar cuidadosamente la necesidad de recolectar evidencia digital relevante con el derecho a la privacidad de individuos que pueden no estar directamente implicados en un delito.

La defensa frecuentemente impugna la admisibilidad de evidencia digital, cuestionando la forma en que fue obtenida, preservada o analizada. Es esencial que los investigadores sigan las mejores prácticas y estándares técnicos para que las pruebas presentadas en juicio no sean descartadas por motivos procedimentales.

Entonces algunos desafíos podrían enunciarse:

- La admisibilidad en los tribunales: la evidencia digital debe cumplir con ciertos requisitos para ser admisible. Por ejemplo, debe ser relevante, confiable y admisible bajo las leyes aplicables.
- La preservación de la cadena de custodia: la cadena de custodia es el registro de quién ha tenido acceso a la evidencia y cómo se ha almacenado. Es importante preservarla para garantizar su admisibilidad.
- El acceso a la evidencia: en algunos casos, puede ser difícil acceder a la evidencia digital. Esto puede deberse a que la evidencia se encuentra en un servidor remoto (inclusive fuera de la jurisdicción) o que está protegida por contraseñas.
- La privacidad de los datos: la evidencia digital puede contener información personal que está protegida por la ley. Es importante proteger la privacidad de los datos al recopilar y almacenar evidencia digital.
- La seguridad de la evidencia: la evidencia digital puede ser vulnerable a ataques cibernéticos. Es importante tomar medidas para proteger la seguridad de la evidencia digital.

Los desafíos de privacidad de la evidencia digital incluyen:

- La recopilación de datos: la recopilación de datos digitales puede ser invasiva de la privacidad. Es importante que las personas sean conscientes de cómo se recopilan y utilizan sus datos digitales.
- El uso de datos: los datos digitales pueden ser utilizados para crear perfiles de personas. Estos perfiles podrían utilizarse para fines de *marketing* o para discriminar a las personas.
- El acceso a datos: los datos digitales pueden ser accedidos por terceros sin el consentimiento de la persona. Esto puede ser un riesgo para su privacidad.
- Allanamiento remoto: cuando el allanamiento se realiza de forma remota, no siempre es necesario obtener una orden judicial ya que no hay un impedimento físico. En algunos casos, las fuerzas de seguridad pueden acceder a la evidencia digital sin una orden judicial si tienen una sospecha razonable de que se está cometiendo un delito. También deberá tenerse en cuenta el riesgo en la demora y actuar de manera rápida para obtener resultados que ayuden a la investigación, ya que los procesos judiciales en algunos casos son extensos y la información es de muy fácil eliminación y/o alteración. Esto puede dar lugar a un conflicto entre la necesidad de proteger la privacidad de los usuarios y la necesidad de investigar el cibercrimen.

Para abordar los desafíos legales y de privacidad de la evidencia digital, se necesitan soluciones que garanticen la admisibilidad de la evidencia, la protección de la privacidad y la seguridad de los datos.

Algunas soluciones posibles incluyen:

- Desarrollar definiciones claras de evidencia digital: esto ayudaría a los tribunales a determinar si un tipo de información particular califica como evidencia digital.
- Establecer estándares para la admisibilidad de la evidencia digital: esto ayudaría a garantizar que la evidencia digital sea admisible en los tribunales.
- Desarrollar herramientas para preservar la cadena de custodia de la evidencia digital: esto ayudaría a garantizar que la evidencia digital sea admisible en los tribunales.
- Desarrollar herramientas para acceder a la evidencia digital: esto ayudaría a garantizar que las personas tengan acceso a la evidencia digital que les pertenece.
- Desarrollar herramientas para proteger la privacidad de los datos digitales. Esto ayudaría a proteger la privacidad de las personas.
- Establecer protocolos nacionales y/o provinciales para adquisición de evidencia digital remota

LA JUSTICIA DE SALTA

En este contexto, la Ley Nº 8386[5] de la Provincia de Salta, sancionada en 2023, representa un avance importante en la regulación del allanamiento remoto en Argentina. Esta ley establece la necesidad de una orden judicial para la realización del allanamiento remoto, definiendo requisitos específicos para la emisión de la orden, así como límites y garantías para el investigado. La ley también establece la necesidad de justificar la proporcionalidad y la necesidad de la medida, así como la obligación de control judicial y la comunicación de la medida al imputado.

Sin embargo, la ley de Salta se centra en la investigación de delitos de especial gravedad.

Es necesario que el Congreso Nacional apruebe una ley federal sobre allanamiento remoto, que armonice los distintos marcos legales provinciales y establezca un sistema nacional de control y garantías. La armonización de la normativa provincial, a través de una ley federal, permitirá asegurar una aplicación uniforme del allanamiento remoto en todo el país, garantizando la protección de los derechos individuales y la eficacia de la lucha contra el crimen.

PROBLEMAS GUBERNAMENTALES

Los gobiernos enfrentan grandes desafíos para mantenerse al día con los rápidos y dinámicos cambios tecnológicos que también impactan al mundo del cibercrimen. La continua innovación en medios digitales, redes sociales, comunicaciones móviles, inteligencia artificial y computación en la nube genera nuevos escenarios que los marcos legales tradicionales no alcanzan a contemplar.

Por ejemplo, las fuerzas policiales y de seguridad deben lidiar con nuevas modalidades de *phishing, ransomware, grooming,* sextorsión, espionaje industrial, ataques de denegación de servicio, entre otras. Los ciberdelincuentes migran rápidamente entre plataformas y aplicaciones, aprovechando vacíos legales y el dinámico cambio tecnológico.

Los gobiernos deben invertir en capacitación permanente de fiscales, investigadores y jueces para que comprendan las implicancias técnicas y legales de las innovaciones tecnológicas. También es clave destinar recursos para que las fuerzas de seguridad cuenten con equipamiento, software e infraestructura adecuados para la investigación forense digital.

Asimismo, se requiere una constante actualización de leyes, regulaciones y convenios de cooperación internacional para acotar los espacios de impunidad. Homologar estándares probatorios y agilizar asistencias judiciales recíprocas para obtener evidencia digital en tiempo real resulta vital en esta nueva era.

En definitiva, los gobiernos deben hacer

grandes esfuerzos e inversiones para no quedar rezagados. Deben acompañar la acelerada transformación tecnológica con políticas públicas integrales para enfrentar al siempre innovador cibercrimen.

COOPERACIÓN TRANSNACIONAL

Algunos de los principales mecanismos de cooperación transnacional que existen actualmente para combatir el cibercrimen son:

- Convenio sobre Ciberdelincuencia del Consejo de Europa (Convention on Cybercrime - Budapest, 2001): establece estándares comunes para legislar sobre delitos informáticos e impulsa la cooperación internacional entre países firmantes.
- Red 24/7 de la Convención sobre Ciberdelincuencia[6]: permite intercambios rápidos entre puntos de contacto para asistencia mutua e investigaciones conjuntas.
- INTERPOL[7]: posee una unidad especializada en ciberdelincuencia que brinda soporte a investigaciones e impulsa operaciones coordinadas entre países.
- Europol[8]: agencia de la Unión Europea que asiste a países miembros en investigaciones sobre cibercrímenes mediante análisis e intercambio de información.
- Ameripol[9]: mecanismo de cooperación policial de países americanos que incluye grupos de trabajo sobre delitos cibernéticos.
- Acuerdos de asistencia legal mutua: permiten compartir en tiempo real evidencia digital entre fiscalías/tribunales con distintos alcances según los países.
- Equipos conjuntos de investigación: unidades conformadas por varios países para cooperar en casos específicos de ciberdelincuencia transnacional.
- Centros de respuesta a incidentes (CSIRTs): red global de equipos que colaboran para responder a ciberataques y compartir información.

Aunque persisten desafíos, estos mecanismos buscan mejorar la coordinación transfronteriza para perseguir de manear más eficaz, a las sofisticadas redes criminales *online* globalizadas.

PANORAMA DE ARGENTINA

En comparación con otros países del mundo, Argentina presenta algunos aspectos positivos que se detallan a continuación, pero aún persisten desafíos en su lucha contra el cibercrimen:

Aspectos positivos:

- Tipificó varios delitos informáticos en su Código Penal, como fraudes, daños informáticos y *grooming* (Arts 77, 128, 131, 153, 155, 157, 173, 183, 184, 197 y 255).
- Creó fiscalías especializadas en ciberdelincuencia a nivel federal y en algunas provincias.
- Es parte de la Convención de Budapest sobre Ciberdelincuencia[10], desde 2017.
- Ha realizado numerosas operaciones coordinadas con INTERPOL en materia de pornografía infantil online[11].
- Cuenta con un CERT[12] (Computer Emergency Response Team) que alerta sobre incidentes y amenazas cibernéticas.

Principales desafíos:

- Falta actualizar los códigos procesales para investigar eficazmente ciberdelitos.
- Escasez de recursos y capacitación a fuerzas de seguridad, operadores judiciales, fiscales y jueces en evidencia digital.
- Limitada cooperación internacional en tiempo real para obtener pruebas digitales.
- Insuficientes campañas de prevención y concientización sobre riesgos cibernéticos.
- Necesidad de más centros asistenciales a víctimas de ciberdelitos.

Si bien Argentina ha dado pasos importantes, sigue estando muy por detrás de países más avanzados en ciberseguridad como Estados Unidos, Reino Unido, Francia o Corea del Sur. Se

debería redoblar esfuerzos y afrontar con seriedad para fortalecer sus capacidades legales, técnicas e institucionales frente al cibercrimen.

CONCLUSIÓN

La investigación forense digital enfrenta desafíos complejos en la era actual: explosiones de datos, amenazas cibernéticas y redes criminales globales. Pero los investigadores cuentan con más y mejores herramientas. Con adecuados recursos, capacitación e intercambio internacional de evidencias, se puede aprovechar el potencial de la información digital para esclarecer todo tipo de crímenes.

Deben crearse los mecanismos de cooperación transnacional para adaptar los procesos legales y técnicas de investigación a esta nueva realidad. Armonizar estándares probatorios y mejorar la asistencia legal mutua resultarán aspectos centrales en esta nueva etapa. Solo así se podrá enfrentar con éxito a las innovadoras modalidades del cibercrimen contemporáneo.

BIBLIOGRAFÍA

1- Ministerio de Seguridad. [07/06/2016]. Resolución 234/2016. Protocolo General de Actuación para las fuerzas policiales y de seguridad en la investigación y proceso de recolección de pruebas en ciberdelitos https://servicios.infoleg.gob.ar/infolegInternet/anexos/260000-264999/262787/norma.htm

2- Ministerio de Seguridad. [2021-11-26]. Resolución 528/2021. Protocolo de actuación para la investigación científica en el lugar del hecho. https://servicios.infoleg.gob.ar/infolegInternet/anexos/355000-359999/357248/norma.htm

3- Ministerio de Seguridad. [17/04/2023]. Resolución 232/2023. Protocolo para la identificación, recolección, preservación, Procesamiento y presentación de evidencia digital https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-232-2023-382307/texto

4- Seagate Technology. (2017). Data Age 2025 [Infografía]. https://www.seagate.com/files/www-content/our-story/trends/files/data-age-2025-infographic-2017.pdf

5- Senado y Cámara de Diputados de la provincia de Salta. [09/08/2023]. Expte. Nº 91-47.608/23. LEY Nº 8386. https://boletinoficialsalta.gob.ar/instrumento.php?cXdlcnR5dGFibGE9THw4Mzg2cXdlcnR5

6-Organización de los Estados Americanos. (2020). Red Interamericana de Cooperación en materia de Ciberseguridad (Ciber Red) [Informe]. https://www.oas.org/juridico/spanish/cyber/cyb20_network_sp.pdf

7-Interpol. (s. f.). Ciberdelincuencia. Interpol. Recuperado [01/12/2023] de https://www.interpol.int/es/Delitos/Ciberdelincuencia

8-Interpol. (s. f.). Ciberdelincuencia. Interpol. Recuperado [Fecha en que accediste al sitio web] de https://www.interpol.int/es/Delitos/Ciberdelincuencia/

9-Infobae. (2023, 9 de noviembre). Ameripol: la nueva herramienta de América Latina y el Caribe contra el crimen organizado. https://www.infobae.com/america/agencias/2023/11/09/ameripol-la-nueva-herramienta-de-america-latina-y-el-caribe-contra-el-crimen-organizado/

10-Congreso de la Nación Argentina. [27/10/201]. Ley 27411. Convenio sobre ciberdelito del Consejo de Europa. https://www.argentina.gob.ar/normativa/nacional/ley-27411-304798

11-Interpol, (2013, 4 de diciembre). Una operación apoyada por INTERPOL para combatir la distribución de pornografía infantil en línea da lugar a detenciones en toda América Latina. https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2013/Una-operacion-apoyada-por-INTERPOL-para-combatir-la-distribucion-de-pornografia-infantil-en-linea-da-lugar-a-detenciones-en-toda-America-Latina

12-Jefatura de Gabinete de ministros. (s. f.). Misiones y funciones del CERT.ar. Argentina.gob.ar. [01/12/2023]. https://www.argentina.gob.ar/jefatura/innovacion-publica/ssetic/direccion-nacional-ciberseguridad/cert-ar/misiones-y-funciones-del