Themis

Recibido: junio/2025
Aceptado setiembre/2025

Revista de la Facultad de Ciencias Jurídicas
de la Universidad Católica de Salta (Argentina)

Argentina y su asignatura pendiente: ciberseguridad

Argentina and its pending subject: cybersecurity

Gonzalo Emanuel Molinati [1]

Resumen

Este trabajo analiza cómo el avance vertiginoso de la tecnología ha generado nuevas formas de criminalidad que desbordan el Código Penal argentino, lo que evidencia vacíos normativos críticos. A través de casos concretos y estadísticas actualizadas, se expone la insuficiencia del marco legal vigente, la falta de preparación y la debilidad de las políticas públicas. Asimismo, se aborda el complejo debate sobre el anonimato en las redes digitales, al defender su relevancia como una garantía democrática esencial para la protección de la libertad de expresión, en especial en contextos de vulnerabilidad y disidencia política. Se advierte que los intentos simplistas de eliminar el anonimato pueden presentar consecuencias negativas para los derechos fundamentales.

El trabajo sostiene que el derecho penal debe reformarse a fin de enfrentar los desafíos del delito digital, mediante una normativa dinámica, instituciones fortalecidas, cooperación internacional y políticas públicas sostenidas. No obstante, el abordaje se realiza desde el campo del derecho penal y la política criminal, sin pretensión de agotar los aspectos técnicos propios de la informática o la ciberseguridad. Las fuentes utilizadas (normativas, jurisprudenciales, doctrinarias y periodísticas) provienen de documentos públicos, medios de comunicación reconocidos, producciones académicas y registros oficiales.

Palabras clave: delitos; tecnología; legislación; privacidad; ciberseguridad

Abstract

This paper analyzes how the rapid advancement of technology has generated new forms of criminality that go beyond the scope of the Argentine Criminal Code, revealing critical regulatory gaps. Through concrete cases and up-to-date statistics, it exposes the insufficiency of the current legal framework, the lack of preparedness, and the weakness of public policies. It also addresses the complex debate surrounding anonymity in digital networks, defending its relevance as an essential democratic guarantee for the protection of freedom of expression, especially in contexts of vulnerability and political dissent. It warns that simplistic attempts to eliminate anonymity may have negative consequences for fundamental rights.

The paper argues that criminal law must be reformed to meet the challenges of digital crime through dynamic legislation, strengthened institutions, international cooperation, and sustained public policies. However, the approach is taken from the field of criminal law and criminal policy, without aiming to cover the technical aspects specific to computer science or cybersecurity.

The sources used—normative, jurisprudential, doctrinal, and journalistic—come from public documents, reputable media outlets, academic publications, and official records.

Keywords: Crimes; technology; legislation; privacy; cybersecurity

Derecho/ ensayo

Citar: Molinati, G. E. (2025). "Argentina y su asignatura pendiente: ciberseguridad". *Themis*, 2 (2), pp. 31-42.

[1] Universidad Católica de Salta

INTRODUCCIÓN

La informática es la disciplina que se ocupa del tratamiento automático de la información mediante dispositivos digitales. En ese contexto, la ciberseguridad tiene como objetivo proteger los sistemas informáticos de cualquier ciberamenaza (IBM, 2024). Este campo no solo abarca cuestiones técnicas, sino también jurídicas, organizacionales y sociales.

En la actualidad, muchas actividades que antes se ejecutaban de manera manual se rinden ante la tecnología; lo que antes requería fuerza material hoy puede realizarse a través de un dispositivo. Este avance ha propiciado el surgimiento de nuevos comportamientos disvaliosos[2], que en muchos casos desbordan las categorías del derecho penal. Lo que en otra época se consideraba ciencia ficción, hoy es parte de la realidad, una realidad que ya no puede considerarse sorprendente ni novedosa.

> Ya no es posible afirmar que los delitos informáticos son algo novedoso o un fenómeno al cual deberíamos mostrarnos con asombro. Al menos no debería ser así para aquellos que se encuentran cercanos al mundo de la tecnología o, incluso, vinculados al ámbito del derecho penal. (Temperini, 2018, p. 52)

Durante 2023, Argentina registró un promedio aproximado de dos mil cincuenta y tres ataques cibernéticos por semana, lo que equivale a cerca de doscientos noventa y tres incidentes diarios (Check Point Research, 2023, citado en iProUP, 2023). Con el objetivo de dimensionar la magnitud de estos delitos, se estima que si el cibercrimen se considerara un Estado nación, constituiría la tercera economía más grande del mundo (Cybersecurity Ventures, 2023).

A la luz de estos datos, el principio de legalidad, el cual exige que los delitos y las penas estén definidos en una ley previa de manera clara y precisa, enfrenta un serio desafío. Las reformas más significativas en la materia (Leyes 26.388 y 26.904), si bien representaron avances en su momento, hoy resultan insuficientes frente al creciente nivel de las amenazas digitales.

El marco legal actual comprende el Código Penal y las normas conexas, la Ley 26.388 amplió el título penal con tipificaciones adaptadas, por ejemplo, delitos de pornografía infantil en Internet (art. 128 CP), interceptación de comunicaciones (art. 153. CP), acceso no autorizado a sistemas (art. 153 bis CP), acceso y alteración de bases de datos personales (art. 157 bis CP), fraude informático (art. 173 inc. 16 CP) y daño informático (art. 183 y 184 CP). La Ley 26.904 definió y sancionó el *grooming* (art. 131 CP) y, además, la Ley 25.326 de *habeas data,* que protege datos personales, tipificó infracciones informáticas.

VACÍOS LEGALES Y NUEVAS AMENAZAS DIGITALES

Diversas prácticas delictivas no se encuadran en este marco legal como figuras autónomas y desbordan los límites del Código Penal, lo que provoca una respuesta legal fragmentaria e ineficaz.

Tal es el caso del *ransomware*, un *software* malicioso que restringe el acceso a archivos de una computadora, que exige un rescate económico a cambio de restaurarlo. Un ejemplo ocu-

[2] Comportamientos disvaliosos: término jurídico que refiere a conductas reprochables o dañinas, aunque no todas estén necesariamente tipificadas como delito.

rrió el 7 de junio de 2023: la Comisión Nacional de Valores sufrió un ataque de este tipo. El grupo Medusa secuestró sus sistemas y robó 1,5 terabytes de información, tras lo cual exigió un rescate de 500.000 dólares. Ante dicha situación, la CNV decidió no pagar el rescate, lo que provocó que los atacantes publicaran parte de la información robada en la *dark web* (Meaños, 2023).

Esta conducta no se encuentra tipificada de manera autónoma en el ordenamiento jurídico argentino. Podría intentar encuadrarse en el delito de sabotaje informático (art. 183, segundo párrafo, CP), que prevé una pena de quince días a un año, claramente desproporcional para un ataque que puede afectar servicios públicos, base de datos, incluso el sistema financiero nacional. También se podría buscar encuadrar en el delito de extorsión (art. 168 CP), que sí contempla una pena más elevada de cinco a diez años de prisión. Lo cierto es que este tipo de delito requiere una intimidación directa o violencia, elementos que en los ataques de *ransomware* muchas veces no están, donde la amenaza suele ser anónima, generalizada y sin contacto personal con la víctima.

Otra modalidad en ascenso es el *phishing*, el cual tiene como objetivo engañar al destinatario mediante correos electrónicos, mensajes o sitios web falsos, para que realice una acción y así revelar información financiera, credenciales de acceso u otra información sensible. Este tipo de delitos presenta un crecimiento continuo. Para el año 2023, estos ataques crecieron un 40 % respecto del periodo anterior, del 1 de abril de 2022 al 31 de marzo de 2023 (Unidad Fiscal Especializada en Ciberdelincuencia [UFECI], 2023). Pese a su expansión, esta modalidad tampoco se encuentra tipificada como delito autónomo, y la sustracción de estos datos no constituye un delito por sí misma, porque la acción de *phishing* en sí no es delito, sino hasta que se comete un fraude concreto,, lo que provoca que la función preventiva del derecho penal se vea frustrada.

A estos se suman fenómenos recientes como el *doxing* o la difusión maliciosa de datos privados. Como reconoció el Ministerio de Justicia (marzo de 2025), "no existen leyes *antidoxing* específicas en Argentina", y su legalidad se determinará en el caso concreto y si coexiste con figuras penales como amenazas, acoso o violación de privacidad.

También se encuentran los *deepfakes* sexuales (videos, imágenes o audios generados por inteligencia artificial que imitan la apariencia y la voz de una persona con tal precisión que pueden engañar) y la pornovenganza (difusión no consentida de imágenes con contenido sexual explícito o sugerente). La legislación solo penaliza estas conductas cuando la víctima es menor de edad. Por lo tanto, en el caso de adultos se debe recurrir a figuras indirectas.

En la actualidad, existen varios proyectos de reforma en marcha; el más abarcativo se trata del presentado por el Ministerio de Justicia de la Nación en marzo de 2025, que propone la modificación integral del Código Penal para incorporar la tipificación autónoma de conductas como las ya nombradas, la criminalización de la difusión de datos personales peligrosos y el fortalecimiento de otras figuras ya reguladas. No obstante, hasta la fecha, ninguna propuesta ha sido sancionada aún como ley. El proceso legislativo avanza con lentitud, lo que es muy habitual en muchas propuestas anteriores tras haber perdido el estatus parlamentario sin tratamiento.

En síntesis, los vacíos normativos existentes demandan una necesaria transformación del derecho penal orientada a anticipar y contener las nuevas formas de ataque digital. Este escenario otorga la oportunidad de construir un ordenamiento jurídico dinámico, efectivo y equilibrado, capaz de proteger a la sociedad.

El derecho no puede permanecer rígido e insuficiente mientras el delito se multiplica y se perfecciona en el ciberespacio.

ANONIMATO EN REDES

Este análisis nos conduce al debate del anonimato en el entorno digital. Para empezar, sería incorrecto pensar que los delitos informáticos más graves se cometen a través de redes sociales comunes. En la práctica, los actores operan mediante canales encriptados[3], *dark web*[4] o a través de *proxies*, VPN[5] y otros mecanismos de evasión que escapan del radar. Eliminar el anonimato en redes sociales o foros públicos no afectaría de manera sustancial a la cibercriminalidad; en cambio, podría restringir la libertad de expresión de millones de personas que no cometen delito alguno.

El anonimato también es una herramienta utilizada por aquellos que desean proteger su identidad con razones legítimas, como el temor al acoso, las amenazas o las represalias políticas. Periodistas, denunciantes, sobrevivientes de abusos sexuales o violencia de género e incluso ciudadanos comunes necesitan expresarse sin miedo. El anonimato es la continuación moderna del derecho humano a la expresión sin coacción, consagrado en los art. 12 y 19 de la Declaración Universal de Derechos Humanos. (Naciones Unidas, 1948).

Cabe destacar que el resguardo de identidad antecede a Internet. A lo largo de la historia, se han publicado obras firmadas con seudónimos y escritos anónimos que impulsaron revoluciones y denuncias por corrupción.

Un ejemplo emblemático son *The Federalist Papers*, ochenta y cinco ensayos escritos por James Madison, Alexander Hamilton y John Jay entre 1787 y 1788 en el anonimato, bajo el seudónimo común "Publius"[6]. George Washington apoyó la transmisión y la difusión de estos borradores con el objetivo de que pudieran publicarse y distribuirse a gran escala. Se consideran una de las obras más importantes de la filosofía política estadounidense (Mount Vernon Ladies' Association, s.f.).

En tiempos recientes, y bajo el argumento de combatir discursos de odio, distintos sectores políticos promovieron proyectos a fin de eliminar el anonimato en redes sociales, lo que obliga a verificar identidades o etiquetar cuentas. Si bien la preocupación por el abuso es válida, las medidas no se enfocan en resolver el problema real. La disidencia política no puede encasillarse como "odio", sin caer en riesgo de criminalización del pensamiento diferente.

La Corte Suprema de Justicia de la Nación ha establecido jurisprudencia en el fallo Servini de Cubría. María Romilda s/ amparo (S. 303- S. 292), en voto del Dr. Boggiano, que "el honor y la intimidad de las personas no admiten, como regla, protección judicial

[3] Canales encriptados: medios de comunicación digitales que usan técnicas de cifrado para proteger el contenido de mensajes y llamadas.

[4] Dark web: parte oculta de internet que no es accesible mediante buscadores convencionales y que requiere software especial para acceder.

[5] *Proxies* y VPN: servicios que permiten modificar u ocultar la dirección IP del usuario para navegar de forma anónima o desde otra ubicación.

[6] *Publius* fue en honor a Publius Valerius Publicola, un estadista romano del siglo V a.C. famoso por ser uno de los fundadores de la República Romana.

preventiva, sino remedios reparatorios" (Corte Suprema de Justicia de la Nación, 1992). Por ello, se debe actuar con suma cautela y de manera excepcional, con el objetivo de no vulnerar los derechos ni las garantías constitucionales.

Además, el anonimato en la red es débil y reversible. Una cuenta puede vincularse a una persona mediante el rastreo de IP[7], datos de registro, con una simple orden judicial dirigida al proveedor de servicios. No se trata de un anonimato impenetrable, sino de una capa de privacidad legítima, cuya vulneración requiere control judicial.

Exigir una identificación no evitaría la comisión del delito, sino que desalentaría la participación de personas legítimamente vulnerables. Lo que resulta aún más problemático es que permite el uso discrecional de los datos por parte del poder político o corporativo.

En nuestra sociedad, la expresión de ideas no requiere la acreditación de identidad ni la firma previa de declaración alguna. Es cierto que el anonimato puede facilitar comportamientos abusivos, pero la respuesta no radica en su eliminación. Las plataformas cuentan con herramientas a fin de moderar contenidos y sancionar a cuentas que violen normas, que son suficientes para actuar en la mayoría de los casos sin necesidad de caer en un régimen policial de identidad digital.

Ceder ante soluciones simplistas puede implicar perder mucho más que el derecho a callar un insulto; puede ser el primer paso con el propósito de silenciar el pensamiento crítico, suprimir voces incómodas y renunciar a los espacios seguros que hacen posible la disidencia, la denuncia y la expresión libre.

RESPONSABILIDAD INSTITUCIONAL

Es importante aclarar que la responsabilidad institucional frente al avance del delito es ineludible. El problema no solo se limita a una cuestión normativa, sino también a la capacidad de respuesta y a la organización técnica. En numerosos casos, tanto entidades públicas como privadas evidencian una profunda desidia o incompetencia técnica frente a vulnerabilidades de seguridad, al ignorar o al desestimar advertencias legítimas. Esta deficiencia estructural no solo refleja una falta de preparación, sino también una preocupante desconexión con los estándares internacionales de ciberseguridad.

Un caso ilustrativo es el de Gaspar Ariel Ortmann, quien, en 2019, mediante técnicas específicas, detectó una vulnerabilidad en su cuenta de banca por internet del Banco Nación. Aprovechó el fallo a fin de operar con una cotización del dólar errónea. La operación se efectuó con una cotización de compra de ARS 5.695 (cuando la real era de ARS 56,95) y luego vendiéndolos a ARS 530,50 (cuando la real era de 53,05), con lo que alcanzó un monto total de USD 11.800. En octubre se presentó de manera personal al banco a fin de mostrar pruebas en referente a lo sucedido y en su declaración, Ortmann sostuvo que "desde que detectó el problema de seguridad, intentó comunicarse con los responsables de los sectores correspondientes mediante todas las formas que se encontraban a su alcance: redes sociales, teléfonos, WhatsApp, correos electrónicos, y sin recibir respuesta.". Por último, el 23 de octubre de 2019, presentó por medios físicos una nota al banco, que tampoco tuvo respuesta. "Nunca recibí una respuesta. Como no tengo intenciones de usar ese dinero ni quiero tener

[7] IP (Protocolo de Internet): identificador numérico único asignado a cada dispositivo conectado a una red informática que utiliza el protocolo IP, como Internet. Permite localizar y distinguir equipos en la red.

problemas, decidí dejarlo en mi cuenta sin tocar nada", testificó Ortmann. (La Nación, 2020).

Este caso se valoró de manera favorable, ya que permitió identificar fallas en la seguridad y culminó con el sobreseimiento de Ortmann por parte del Juzgado Federal N.º 1, a cargo del juez Marcelo Martínez de Giorgi (Juzgado Federal N.º 1 de CABA, 2020; La Nación, 2020).

Más allá del fallo, el hecho evidencia una falta de gestión institucional, lo que demuestra incluso cómo muchas veces el Estado no cuenta con canales adecuados a fin de recibir alertas éticas de seguridad digital. En contraste, en el ámbito privado a nivel global, canalizar estos reportes a través de programas especializados es una práctica común e incluso cuentan con sistemas de recompensa (bug bounty8) con el objetivo de incentivar la colaboración ciudadana en la protección de los sistemas críticos.

EVIDENCIA DIGITAL Y DEBILIDADES DEL SISTEMA JUDICIAL

Esta falta de infraestructura técnica e institucional para gestionar de manera adecuada la ciberseguridad muchas veces se replica en el plano judicial. Un caso paradigmático ocurrió en la provincia de Mendoza, en el marco de la causa contra el juez federal Walter Bento, tramitada ante el Tribunal Oral Federal N.º 2. Según la denuncia pública realizada en una publicación de Instagram por el canal especializado Derecho Informático (a cargo del perito informático Leandro Suárez) el Cuerpo de investigaciones y la Fiscalía habrían incorporado a un expediente penal un informe técnico basado en capturas de pantalla, que solo se limitaron a imprimir, sin haber efectuado copias forenses del dispositivo ni generado el correspondiente código *hash*[9]. (Suárez, 2025)

Esta exigencia no es opcional ni excesiva, ya que contradice de modo expreso lo establecido por la *Guía de obtención, preservación y tratamiento de evidencia digital*, presentada y aprobada en el marco de la XVII Reunión Especializada de Ministerios Públicos del Mercosur, la cual exige que toda imagen forense incorpore un cálculo *hash*.

> Calcular el *hash* de la copia forense permitirá verificar si la misma fue alterada con posterioridad a su obtención. Si pasado un tiempo de realizada la misma, alguien plantea que fue alterada, bastará calcular el *hash* para ver si el contenido es el mismo del originalmente obtenido (en este caso, se demuestra que la copia no fue manipulada). (Procuración General de la Nación, 2016)

Conforme a lo señalado con anterioridad, en la causa n.º 41459/2019-3 de la Ciudad Autónoma de Buenos Aires, la Cámara de Apelaciones analizó una situación análoga, donde se debatió la validez de una captura de pantalla de un teléfono celular como prueba de un caso de contacto con menores por redes sociales. Si bien la mayoría del tribunal convalidó su uso al alegar que el error se había subsanado, el voto disidente del juez Sergio Salgado advirtió que la admisión de una prueba sin adecuada preservación digital vulnera derechos de jerarquía constitucional.

[8] *Bug bounty*: programa en el que empresas u organizaciones ofrecen recompensas económicas a investigadores o *hackers* éticos que descubren y reportan vulnerabilidades

[9] *Hash*: secuencia de caracteres generada a partir de un dato mediante una función matemática específica. Esta secuencia actúa como una especie de "huella digital", si el dato se modifica, aunque sea mínimamente, el hash resultante será completamente distinto.

> …no puede más que concluirse que podrían estar siendo vulnerados derechos de raigambre constitucional del encausado como son la defensa en juicio, el debido proceso y el principio de inocencia, y que, por lo tanto, el gravamen que se le estaría irrogando sería de imposible reparación ulterior, dado que se cuestiona una decisión que admite someterlo a juicio en base con una prueba que, se alega, no ha sido preservada conforme a derecho. (Cámara de Apelaciones en lo Criminal y Correccional de la Ciudad Autónoma de Buenos Aires, Sala I, 2021, p. 3)

Si bien en principio podría parecer una mera omisión técnica, el juez interviniente indicó con acierto que dicha falencia implica una seria vulneración de principios de jerarquía constitucional.

No se trata de hechos aislados, sino de un déficit estructural en la gobernanza tecnológica del Estado. Lejos de ser un error menor, este tipo de prácticas frustra el desarrollo adecuado de los procesos penales, lo que compromete la obtención de pruebas válidas, afecta la eficacia investigativa y debilita las garantías propias del debido proceso.

LA POLÍTICA CRIMINAL FRENTE A LA CIBERSEGURIDAD

En tanto, la política criminal a nivel nacional tampoco cambia de manera sustancial. Un informe reciente de la organización Derechos Digitales destaca que en Argentina, si bien pareciera existir una estrategia nacional definida, escasean recursos tanto técnicos como humanos (Derechos Digitales, 2024, p. 5).

La Agencia Federal de Ciberseguridad (AFC), creada en 2024 dentro de la órbita de la SIDE, representa un primer paso en el reconocimiento institucional del problema y apunta a ordenar un ecosistema fragmentado. Sin embargo, a poco de su puesta en marcha, las propias autoridades reconocían limitaciones estructurales críticas, ya que explican que no alcanza "ni para el equipamiento básico". En palabras de un funcionario: "Tuvimos menos presupuesto que un banco chico para asegurar al país" (Brodersen, 2025).

En 2025, se aprobó el Plan Federal de Prevención de Ciberdelitos y Gestión Estratégica de la Ciberseguridad 2025-2027 mediante la Resolución 72/2025, publicada en el Boletín Oficial (Resolución 72/2025, 2025). El plan involucra a todas las fuerzas federales y extiende su alcance a las provincias y a la Ciudad Autónoma de Buenos Aires. Busca desarrollar protocolos comunes para el abordaje de incidentes, promover capacitación técnica y fomentar la cooperación federal.

Por primera vez, se intentó establecer un marco programático con visión federal y multidisciplinaria en la materia. Sin embargo, el propio documento establece que no implicará erogación presupuestaria directa, lo que en la práctica podría traducirse en una escasa capacidad operativa. Asimismo, carece de plazos específicos, indicadores medibles de cumplimiento y rendición de cuentas en un país donde muchos instrumentos legales han quedado sin aplicación.

La ciberseguridad no puede abordarse como un lujo técnico, ni mucho menos relegarse a una oficina con fondos residuales. Es necesario comprenderla y gestionarla de manera adecuada como una política de Estado sostenida en el tiempo, transversal a los Gobiernos y blindada frente a los cambios de administración. Esto implica una estructura dotada de legitimidad, la cual se logra con transparencia; la ciudadanía necesita saber quiénes son los encargados, cómo se toman las decisiones, qué incidentes han ocurrido y qué se lleva a cabo a fin de prevenirlos.

INTEGRACIÓN REGIONAL

Un aspecto fundamental de la ciberdelincuencia es su carácter inherentemente global; su persecución muchas veces requiere colaboración internacional y marcos normativos compatibles entre Estados.

> Otro problema que surge con la tipificación de los delitos informáticos […] es que las leyes penales están normalmente pensadas para ser aplicadas en un Estado determinado, y este tipo de delitos en la mayoría de las ocasiones trasciende las fronteras nacionales. *(*Grenni & Fernández Ríos, 2018, p. 102*)*

En América Latina, si bien se han producido avances relevantes, como la adhesión de varios países al Convenio de Budapest sobre la ciberdelincuencia y la promoción de iniciativas técnicas por parte de la Organización de los Estados Americanos (OEA), la región aún carece de una legislación vinculante y una estrategia común. La falta de una arquitectura integrada dificulta la coordinación entre países.

En contraste, la Unión Europea ha consolidado un modelo avanzado. Mediante la Directiva NIS 2 (2022/2555) se estableció un marco legal unificado a fin de mejorar la ciberseguridad en sectores críticos, tanto privados como públicos, al igual que en los sectores de energía, transporte, salud, finanzas y servicios digitales. Establece la obligación para las entidades de adoptar medidas rigurosas de gestión de riesgos y notificar incidentes dentro de plazos definidos. Además, responsabiliza a la alta dirección por el cumplimiento de estas, al imponer sanciones en su caso. Articula también redes supranacionales y promueve mecanismos de supervisión y cumplimiento (Parlamento Europeo y Consejo de la Unión Europea, 2022).

Esta comparación revela una disparidad significativa. Con el objetivo de fortalecer la ciberseguridad, es esencial que tanto Argentina como los países de la región avancen hacia mecanismos más sólidos de cooperación internacional, pero, por sobre todo, una integración regional efectiva, que permita el intercambio fluido de información y la coordinación de políticas, con el fin de construir una respuesta más eficiente frente a los riesgos globales del ciberespacio.

HACIA UNA POLÍTICA PENAL DEL SIGLO XXI

Es imprescindible superar la mera descripción crítica y avanzar hacia un enfoque constructivo. El cibercrimen exige respuestas técnicas, jurídicas e institucionales. Algunas líneas de acción indispensables son las siguientes:

Reforma legal dinámica

Se propone una modificación integral del Código Penal que incorpore de forma autónoma delitos sin regulación específica. Sin embargo, más allá de la incorporación puntual de figuras, deben establecerse actualizaciones periódicas que permitan al derecho penal adaptarse a los cambios tecnológicos de forma flexible y sostenida.

Fortalecimiento institucional

La ciberseguridad no puede funcionar como un apéndice burocrático. Se requieren agencias especializadas, con presupuesto propio, autonomía funcional, independencia política y personal técnico altamente calificado.

Capacitación integral del sistema judicial y de seguridad

Es necesaria una formación continua para fiscales, jueces, fuerzas de seguridad y perso-

nal auxiliar. Sin conocimiento técnico adecuado, los procesos se frustran, se pierden pruebas o se vulneran garantías.

Articulación interinstitucional y cooperación internacional

El abordaje del cibercrimen requiere redes de cooperación entre los niveles nacional y provincial, así como con organismos internacionales. Además, es clave generar alianzas con universidades, organismos técnicos y empresas del sector privado para el intercambio de conocimiento y buenas prácticas.

Inversión pública en infraestructura tecnológica

Se deben destinar recursos públicos a la creación de laboratorios forenses digitales, redes de respuesta, sistemas de monitoreo y plataformas seguras que no dependan de los cambios de gestión ni de las coyunturas políticas.

CONCLUSIÓN

Este diagnóstico no debe generar pesimismo, sino impulsar la acción. La magnitud del problema no debe inmovilizarnos, sino convocarnos a pensar un derecho penal que no se limite a intervenir una vez cometido el delito, sino que sea capaz de anticiparlo y contenerlo.

Lo que antes requería armas y fuerza, hoy se consigue con un clic, una brecha o un archivo malicioso. Ya no se necesita romper puertas, solo contraseñas. No se mueve en la oscuridad ni en las sombras, sino en el ciberespacio, donde los atacantes pueden operar desde cualquier parte del mundo.

Argentina, al igual que muchos países, enfrenta el desafío de responder a una criminalidad digital con herramientas obsoletas. El cibercrimen se expande con velocidad, mientras la implementación de la ley parece progresar de manera lenta y la institucionalidad tambalea ante ataques cada vez más sofisticados. Cuando el Estado no está preparado para protegernos, no solo pierde la víctima: pierde el derecho mismo, que ve limitada su eficacia frente a delitos que no sabe nombrar, calificar ni perseguir.

Es tiempo de pensar en una política que no responda desde la improvisación, sino desde el conocimiento, la técnica y el compromiso con una sociedad segura.

REFERENCIAS BIBLIOGRÁFICAS

Argentina.gob.ar. (2025). ¿Qué es el *doxing y cómo podemos cuidarnos?* https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/que-es-el-doxing-y-como-podemos-cuidarnos#:~:text=Si%2C%20no%20existen%20leyes%20antidoxing,seg%C3%BAn%20la%20naturaleza%20del%20caso

Brodersen, J. (2025). *Hackeos al Estado: avances, críticas y qué dicen en la Agencia Federal de Ciberseguridad sobre la estrategia nacional. Brodersen Darknews.* https://www.brodersendarknews.com/p/hackeos-al-estado-criticas-afc-cert-dnc

Cámara de Apelaciones en lo Criminal y Correccional de la Ciudad Autónoma de Buenos Aires, Sala I. (2021). Causa n. º 41459/2019-3 [Fallo]. https://pupilacdn.nyc3.cdn.digitaloceanspaces.com/diariojudicial.public/documentos/000/099/168/000099168.pdf

Check Point Research. (2023, citado por iProUP). *Ciberataques: Argentina sufrió 2.052 ataques semanales en promedio. iProUP.* https://www.iproup.com/innovacion/39852-

ciberataques-argentina-sufrio-2052-ataques-semanales-en-promedio

Corte Suprema de Justicia de la Nación. (1992). Servini de Cubría, María Romilda s/ amparo (S. 303-S. 292) [Fallo]. https://www.saij.gob.ar/corte-suprema-justicia-nacion-federal-ciudad-autonoma-buenos-aires-servini-cubria-maria-romilda-amparo-a92001426-1992-09-08/123456789-624-1002-9ots-eupmocsollaf

Cybersecurity Ventures. (2024). *Cybercrime to cost the world $9 trillion annually in 2024*. https://cybersecurityventures.com/cybercrime-to-cost-the-world-9-trillion-annually-in-2024/

Derechos Digitales. (2024). *Ciberseguridad en América Latina: Estrategias nacionales en 2024*. https://www.derechosdigitales.org/wp-content/uploads/DD_CYRILLA_ESP_2024.pdf

Grenni, L., & Fernández Ríos, R. (2018). La previsión normativa del tipo penal de grooming en la Argentina. En R. A. Parada & J. D. Errecaborde (Eds.), Cibercrimen y delitos informáticos: Los nuevos tipos penales en la era de Internet (pp. 101–120). Erreius.

IBM. (2024). *¿Qué es la ciberseguridad?* https://www.ibm.com/es-es/topics/cybersecurity

Juzgado Federal N.º 1 de la Ciudad Autónoma de Buenos Aires. (2020). Causa Gaspar Ariel Ortmann: sobreseimiento [Fallo]. https://drive.google.com/file/d/16KNmhbhOrA52ucEZ6z3i62_JvEq7O3_h/view

La Nación. (2020). *Hackeó el Home Banking, compró dólares a menor precio y fue sobreseído*. https://www.lanacion.com.ar/sociedad/hackeo-home-banking-compro-dolares-menor-precio-nid2526938/

Meaños, F. (2023, junio 28). *Ciberataque a la CNV: no se pagó el rescate y los hackers liberaron información sensible sobre el mercado. Infobae*. https://www.infobae.com/economia/2023/06/28/ciberataque-a-la-cnv-no-se-pago-el-rescate-y-los-hackers-liberaron-informacion-sensible-sobre-el-mercado/

Mount Vernon Ladies' Association. (s.f.). *The Federalist Papers. Mount Vernon*. https://www.mountvernon.org/library/digitalhistory/digital-encyclopedia/article/federalist-papers

Organización de las Naciones Unidas. (1948). *Declaración Universal de Derechos Humanos*. https://www.un.org/es/about-us/universal-declaration-of-human-rights#:~:text=Art%C3%ADculo%2019,por%20cualquier%20medio%20de%20expresi%C3%B3n

Parlamento Europeo y Consejo de la Unión Europea. (2022). *Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a medidas para un elevado nivel común de ciberseguridad en toda la Unión (Directiva NIS 2)*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555

Procuración General de la Nación. (2016). Guía de obtención, preservación y tratamiento de evidencia digital [PDF]. https://www.fiscales.gob.ar/wp-content/uploads/2016/04/PGN-0756-2016-001.pdf

Suárez, L. [@derechoinformatico]. (2025). *Informe sin HASH [Publicación de Instagram]. Instagram*. https://www.instagram.com/p/DLP_DxHRAOg/

Temperini, M. (2018). Delitos informáticos y cibercrimen: Alcances, conceptos y características. En R. A. Parada & J. D. Errecaborde (Eds.), *Cibercrimen y delitos informáticos: Los nuevos tipos penales en la era de internet* (pp. 33–48). Erreius.

Unidad Fiscal Especializada en Ciberdelincuencia [UFECI]. (2023). *Informe de gestión de la Unidad Fiscal Especializada en Ciberdelincuencia 2022–2023*. https://www.fiscales.gob.ar/wp-content/uploads/2023/12/UFECI_informe-de-Gestion_23_15-12.pdf

Unidad de Información Oficial. (2025). *Plan Federal de Prevención de Ciberdelitos y Gestión Estratégica de la Ciberseguridad 2025–2027* (Resolución 72/2025). https://drive.google.com/file/d/1-iGV_3Cklhjz6yf7hZwXiOQDoXlgl5ea/view

Gonzalo Emanuel Molinati
Perfil Académico y Profesional: Abogado egresado de la Universidad Católica de Salta (UCASAL), con Diplomatura en Derecho Penal (2024). Realizó diversos cursos de práctica profesional y judicial y cuenta con capacitaciones en Inteligencia Artificial y Ciberseguridad aplicadas al derecho. Su interés académico se centra en derecho penal, política criminal y la intersección con la ciberseguridad.
Gonzamolinati@gmail.com
ORCID: https://orcid.org/0009-0006-1089-5807