
DEL TRABAJO DECENTE AL TRABAJO EMERGENTE: LA INTELIGENCIA ARTIFICIAL COMO DERECHO HUMANO

From Decent Work to Emergent Work: Artificial Intelligence as a Human Right

Leonardo Salvador Calvo* y María Paula Carril**

Univ. del Norte Santo Tomás de Aquino / Univ. Católica de Santiago del Estero

leonardosalvadorcalvo@hotmail.com / mpaulacarril@gmail.com

RECIBIDO 17/10/2025 - ACEPTADO 17/11/2025

Resumen

El avance de la inteligencia artificial ha transformado profundamente las condiciones laborales, generando un tránsito del trabajo decente al trabajo emergente. Este artículo analiza cómo la falta de regulación estatal frente a las nuevas tecnologías produce desprotección de derechos fundamentales y amplía la brecha digital. Se propone reconocer el acceso equitativo a la inteligencia artificial como un derecho humano emergente, indispensable para garantizar la igualdad de oportunidades, prevenir nuevas formas de discriminación y asegurar la continuidad del paradigma de justicia social en el mundo del trabajo.

Abstract

The advance of artificial intelligence has profoundly transformed working conditions, marking a shift from decent work to emergent work. This article analyzes how the lack of state regulation regarding new technologies leads to the erosion of fundamental labor rights and deepens the digital divide. It argues that equitable access to artificial intelligence must be recognized as an emerging human right, essential to ensuring equal opportunities, preventing new forms of discrimination, and safeguarding the principles of social justice within the future of work.

Palabras clave:

inteligencia artificial, trabajo decente, trabajo emergente, derecho humano, igualdad.

Keywords:

artificial intelligence, decent work, emergent work, human right, equality.

1. Introducción

La irrupción de la inteligencia artificial (IA) en la vida contemporánea plantea un interrogante que trasciende lo tecnológico: ¿puede considerarse el acceso a estas herramientas como un derecho humano? En las últimas décadas, la humanidad ha presenciado un proceso similar con el acceso a internet, que pasó de ser un privilegio de pocos a ser reconocido internacionalmente como condición indispensable para la educación, el trabajo, la participación democrática y la igualdad social. Hoy, la IA parece recorrer un camino

* Magister en Derecho del Trabajo y Relaciones Laborales Internacionales por la Universidad Nacional de Tres de Febrero. Diplomado en Fundamentos de la Inteligencia Artificial, en Derecho Procesal y Riesgos del Trabajo. Abogado por la Universidad del Norte Santo Tomás de Aquino. Secretario de la Suprema Corte de la Provincia de Jujuy.

** Especialista en Derecho Procesal (UCSE-UNR). Abogada por la UCSE y Diplomada en Derechos Humanos y Control de Constitucionalidad y Convencionalidad por la Universidad de Bolonia. Posgrado en Derecho Laboral por la UBA, Posgrado en Derecho Penal y Diversidad Cultural por la UNJU. Secretaria de la Suprema Corte de Justicia de la Provincia de Jujuy.

análogo, pero con un impacto aún más profundo: no solo organiza la información, sino que interviene en la forma en que producimos, aprendemos, nos comunicamos y participamos en la vida pública.

La aplicación de sistemas automatizados para la toma de decisiones en el ámbito laboral puede derivar en violaciones graves a derechos fundamentales, especialmente cuando no existen mecanismos adecuados de control o transparencia. Como advierte Mario Maldonado Smith, “en el contexto de la cuarta revolución industrial, asistimos a un momento en el que hemos dejado en manos de computadoras decisiones trascendentales, inclusive aquellas que pueden tener incidencia en la tutela y garantía de los derechos humanos” (Maldonado Smith, 2021, p. 72).

Este punto resulta fundamental para comprender la necesidad de reconocer el acceso a la IA como un derecho común a todas las personas. De sus palabras se desprende la urgencia de una regulación específica de esta actividad, cuya vinculación con las nuevas formas de trabajo –propias del denominado trabajo emergente– evidencia la existencia de una laguna normativa que afecta directamente la tutela de los derechos laborales.

En este sentido, Patricia Kurczyn Villalobos advierte que “estos instrumentos, en términos generales, como lo fue en su época la máquina de vapor, sustituyen mano de obra que no debe considerarse como procedimiento de desplazamiento de las personas en el trabajo, ni motor de desempleo. Tampoco es la guerra contra los derechos humanos laborales, de ahí la imperiosa urgencia de regular oportunamente su aplicación y hacer que la ética tenga y mantenga presencia permanente para regular, limitar y evitar excesos innecesarios que puedan dañar a la propia humanidad o tan solo a una persona” (Kurczyn Villalobos, 2023, p. 3).

Resulta suficiente observar las condiciones actuales de acceso al empleo para advertir la consolidación de estrategias de selección mediadas por algoritmos, en las que la utilización de la IA se erige como una herramienta prácticamente indispensable. Este fenómeno evidencia un nuevo filtro tecnológico que condiciona la empleabilidad y tiende a profundizar las desigualdades entre quienes poseen competencias digitales avanzadas y quienes carecen de ellas. En esa línea, como argumenta César Rázuri Vargas (2023, p. 53), “la IA no es una herramienta enemiga de los trabajadores, sino que se muestra como un mecanismo que los Estados deberán emplear, a efectos de que se gesté y promocióne un escenario de empleo digno a nivel global.”

El desafío consiste en precisar la naturaleza de este eventual derecho. Desde un punto de vista estructural, la IA no puede ser comprendida como una mera comodidad tecnológica, sino como un requisito social básico, en tanto condiciona el ejercicio efectivo de otros derechos fundamentales. Quien domina las herramientas de IA accede con ventaja al mercado laboral, a la información, a la educación y a la comunicación; quien no lo hace, corre el riesgo de quedar relegado en una nueva forma de exclusión social.

No es raro ver hoy a las personas –de cualquier rango etario– acceder a la IA para consultas relacionadas con distintas temáticas, para generación de imágenes, adquisición de conocimiento o incluso preguntas de la vida cotidiana; y que esta consulta sea considerada como algo novedoso. Es más, es muy común escuchar a las personas, ante una duda, que alguien sugiera: “preguntale a ChatGPT”. Este fenómeno revela un proceso de naturali-

zación tecnológica que impacta de lleno en la forma en que se conciben el trabajo, la educación y la interacción social.

El presente trabajo propone examinar la IA como un derecho humano emergente y su incidencia directa en el tránsito del trabajo decente al trabajo emergente¹, entendido este último como el conjunto de nuevas realidades laborales surgidas del entorno tecnológico y digital. Desde esta doble perspectiva —ética y jurídica— se abordará el problema de la igualdad en el acceso, los riesgos de exclusión y los fundamentos constitucionales e internacionales que justifican su reconocimiento.

Tal como señalan Milagros Salinas Atencio y Christian Guzmán Napurí (2025, p. 71), “en el área laboral, estos sistemas automatizados se volvieron cruciales al optimizar la selección, valoración y administración del talento humano, no obstante, su uso ha generado preocupaciones marcadas en temas de equidad y transparencia, particularmente por los sesgos algorítmicos que se generan en este proceso de automatización y que pueden resultar en ambientes discriminatorios que pueden manifestarse en la preferencia por ciertos perfiles o en la plena exclusión de determinados grupos vulnerables, suscitando retos para la justicia laboral y la protección de derechos de los trabajadores dado que la falta de regulación perpetúa las desigualdades existentes.”

En definitiva, se pretende demostrar que la IA no solo transforma el modo en que trabajamos, sino también el contenido mismo del derecho al trabajo, obligando a repensar sus estándares de dignidad, equidad y justicia en el contexto de una nueva sociedad digital, donde la equidad tecnológica se convierte en el nuevo parámetro de justicia social.

Este trabajo se inscribe en una línea de investigación más amplia que propone una interpretación dinámica tridimensional del derecho², orientada a ofrecer respuestas hermenéuticas frente a los fenómenos tecnológicos no previstos por el legislador. Sin profundizar aquí en su desarrollo teórico, se adopta su premisa esencial: la necesidad de una interpretación evolutiva que mantenga la vigencia sustantiva de los derechos fundamentales ante el cambio digital.

2. El derecho al trabajo como derecho humano fundamental

El derecho al trabajo constituye uno de los pilares del constitucionalismo social contemporáneo. Su reconocimiento se encuentra consagrado en el artículo 6 primer párrafo del Pacto Internacional de Derechos Económicos, Sociales y Culturales (PIDESC), que establece: “Los Estados Partes en el presente pacto reconocen el derecho a trabajar que comprende el derecho de toda persona de tener la oportunidad de ganarse la vida mediante un trabajo libremente escogido o aceptado, y tomarán medidas adecuadas para garantizar

¹ Esta expresión debe entenderse como el tránsito desde un paradigma laboral consolidado hacia un escenario de transformaciones aún inciertas; del ámbito de lo regulado al de las nuevas realidades tecnológicas todavía no normadas. En definitiva, implica pasar de la estructura conocida del trabajo decente a la apertura dinámica del trabajo emergente, donde el Derecho se ve interpelado a repensar sus categorías tradicionales.

² El método de interpretación dinámica tridimensional ha sido formulado por los autores en un trabajo en elaboración sobre IA y métodos de interpretación de la norma jurídica, en el que se propone un marco hermenéutico integrador entre las dimensiones normativa, sociológica y dikelógica del fenómeno jurídico.

este derecho”. Aquí ya se advierte la obligación de los Estados Partes de adaptar las condiciones de acceso al empleo a los cambios tecnológicos, dentro del marco de las medidas adecuadas que deben adoptar para asegurar el ejercicio efectivo de este derecho.

En el ámbito regional, el art. 26 de la Convención Americana sobre Derechos Humanos (CADH) impone la obligación de desarrollar progresivamente los derechos económicos, sociales y culturales, entre los cuales el trabajo ocupa un lugar central. Como subraya la Corte Interamericana, “esta Corte ha reiterado la interdependencia e indivisibilidad existente entre los derechos civiles y políticos, y los económicos, sociales y culturales” (CIDH, *Lagos del Campo vs. Perú*, párr. 141), y, en esa misma línea, ha resaltado que “[t]oda persona tiene derecho al trabajo en condiciones dignas...” (CIDH, *idem*, párr. 144).³ También, como recuerda la OIT, el trabajo decente implica “trabajo productivo en condiciones de libertad, equidad, seguridad y dignidad, en el cual los derechos son protegidos y que cuenta con remuneración adecuada y protección social.”⁴

Este concepto integrador vincula la noción de trabajo con la justicia social y la inclusión. De ello se desprende que el trabajo no es solo una fuente de ingresos, sino también un espacio de realización humana, que exige condiciones equitativas y seguras. En este sentido, los Estados tienen la obligación no solo de promover el empleo, sino también de garantizar su calidad y accesibilidad, de modo que todas las personas puedan participar del progreso social en igualdad de condiciones. Así, la comprensión del trabajo como derecho humano fundamental constituye el punto de partida para repensar su vigencia y alcance en el contexto del trabajo emergente y de la irrupción de la inteligencia artificial.

3. El derecho humano emergente al acceso equitativo a la IA

3.1. La IA como nueva frontera del desarrollo humano

El Comité de Derechos Económicos, Sociales y Culturales ha subrayado que el derecho a participar en el progreso científico y gozar de sus beneficios implica una obligación estatal activa de garantizar el acceso igualitario y sin discriminación a las aplicaciones de la ciencia. Esta obligación positiva exige la adopción de políticas públicas inclusivas que aseguren la disponibilidad, accesibilidad y participación efectiva de todos los sectores sociales en el uso de nuevas tecnologías, entre ellas la IA, cuyo desarrollo incide directamente en el ejercicio de los derechos económicos, sociales y culturales.⁵

En este marco, hemos señalado la existencia de “lagunas del derecho dinámicas” ante fenómenos tecnológicos de evolución constante, lo que exige respuestas interpretativas acordes, sin alterar la arquitectura constitucional-convencional del sistema (Carril y Calvó, 2025).

La IA, como forma avanzada de dicho progreso, se convierte en una herramienta clave para garantizar el desarrollo humano, la educación continua, el acceso a la información y la empleabilidad en el siglo XXI. En consecuencia, el artículo 15.1.b del PIDESC debe in-

³ Disponible en https://www.corteidh.or.cr/docs/casos/articulos/seriec_340_esp.pdf

⁴ *Memoria del Director General: Trabajo decente*, 87.^a Reunión de la Conferencia Internacional del Trabajo, Ginebra, 1999, pág. 15.

⁵ Paráfrasis del contenido de la *Observación General N.º 25 (2020)* del Comité de Derechos Económicos, Sociales y Culturales, párrs. 15–18, Naciones Unidas, documento E/C.12/GC/25. Disponible en <https://undocs.org/E/C.12/GC/25>

interpretarse evolutivamente: el acceso equitativo a la IA integra el derecho a gozar de los beneficios del progreso científico, en tanto su exclusión implica una restricción indirecta del acceso al conocimiento, al trabajo y a la participación democrática.

3.2. Igualdad material y acceso tecnológico

El avance tecnológico impone a los Estados un deber positivo de prevención y regulación frente a los riesgos inherentes al desarrollo científico y digital. Este deber involucra no solo el entorno ambiental o sanitario sino también el dominio social y laboral, pues la omisión estatal puede consolidar desigualdades estructurales y exclusión digital. Como lo advierte un reciente estudio: “el desarrollo de las nuevas tecnologías (...) no va de la mano con la creación y el desarrollo de los mecanismos de regulación que se necesitan, por lo que resulta preocupante advertir la falta de respuestas por parte de los Estados” (PUCP, 2023).

En el plano práctico, la automatización de los procesos de selección y contratación introduce riesgos de exclusión y afectación de derechos. Como señala Maldonado Smith, “el empleo de los algoritmos aplicado a la fase de contratación laboral plantea muchos aspectos en donde conviene prestar la debida atención. En este caso, la libertad empresarial para la contratación puede encontrarse en tensión frente a derechos fundamentales como la igualdad y la no discriminación, pero también dar margen a la lesión de derechos adicionales como la privacidad, intimidad, la tutela de los datos personales, la tutela judicial efectiva (se recuerde el efecto caja negra), la propia imagen e, incluso, el honor” (Maldonado Smith, *op. cit.*, p. 103).

Asimismo, la igualdad real de oportunidades, prevista en el artículo 75 inciso 23 de la Constitución argentina, obliga a adoptar medidas positivas que aseguren que todos los sectores sociales puedan acceder y utilizar la IA de modo equitativo, evitando que se transforme en un nuevo mecanismo de discriminación socioeconómica. En este sentido, por ejemplo, Kurczyn Villalobos (*op. cit.*, p. 3) enfatiza la obligación de controlar los algoritmos y mantener la justicia algorítmica, que implica eliminar la discriminación algorítmica que el propio ser humano programa.

Tal como hemos sostenido respecto de las relaciones laborales tradicionales, el desequilibrio estructural entre empleador y trabajador justifica un derecho protector. Hoy, ese desequilibrio se reproduce bajo nuevas formas: la asimetría digital, en la que el trabajador desconoce los criterios algorítmicos que rigen su desempeño o selección laboral. En esta línea, Leonardo Stekelberg Poses (2023, p. 3) observa que “se ha hecho hincapié en la necesidad de introducir cambios en la legislación para proteger contra la discriminación (...) que pueda surgir como resultado de la implementación de algoritmos en procesos de toma de decisiones. Existen casos en los que las operaciones digitales pueden ejecutar decisiones discriminatorias, por lo que es fundamental establecer regulaciones que salvaguarden los derechos y eviten prácticas injustas”.

Esta reflexión resulta particularmente relevante para comprender que la desigualdad digital no es solo un problema técnico, sino una cuestión estructural de justicia laboral. La ausencia de mecanismos de control o transparencia en los algoritmos puede transformar la

tecnología en una fuente de exclusión sistemática. Como sugiere Maldonado Smith, “lo preocupante es que, si el algoritmo se encuentra sesgado, la decisión resultante incidiría en los derechos fundamentales, con la agravante de que sería muy difícil de acreditar, colocando al sujeto en una condición de indefensión” (*op. cit.*, p. 96).

3.3. La IA como derecho humano emergente

Podemos definir a estos derechos como aquellos que surgen en respuesta a los desafíos contemporáneos planteados por los avances científicos, tecnológicos y las nuevas formas de exclusión. En ese sentido, entendemos que los derechos humanos emergentes no sustituyen, sino complementan los derechos clásicos, al surgir como consecuencia de la evolución social y tecnológica que genera nuevas necesidades jurídicas y éticas.

En términos del proyecto de Carta de Derechos Emergentes del Instituto de Derechos Humanos de Cataluña, la noción de derechos humanos emergentes “se inscribe como respuesta a los procesos de globalización [que] excluye[n] de sus beneficios a amplias capas de la población mundial”, y advierte, a la vez, “peligros (...) ligados a los avances tecnológicos no controlados” (control/vigilancia, intervención sobre el ser humano).⁶

El acceso equitativo a la IA, aunque no expresamente reconocido, cumple con esos requisitos: su existencia condiciona el ejercicio real de otros derechos humanos reconocidos y constituye una garantía instrumental de igualdad en el mundo digital.

3.4. Obligaciones convencionales de los Estados

Conforme al principio de progresividad (art. 26 CADH y art. 2.1 PIDESC), los Estados deben adoptar medidas legislativas, educativas y presupuestarias para facilitar el acceso equitativo a las tecnologías de IA. La falta de acceso a las tecnologías digitales puede constituir una forma contemporánea de desigualdad y exclusión social. El Comité DESC ha advertido que los Estados deben “promover la ciencia abierta y la publicación en código abierto de las investigaciones” (OG 25, párr. 16).⁷

En consecuencia, los sesgos algorítmicos configuran una nueva forma de discriminación estructural que compromete la obligación estatal de garantizar la igualdad de oportunidades laborales, conforme a los estándares de la OIT y el PIDESC. En otras palabras, el acceso equitativo a la IA no solo es una aspiración ética, sino una obligación jurídica de carácter internacional, derivada de los tratados de derechos humanos vigentes.

En este sentido, César Arese sostiene que “de lo que se trata es de crear antídotos frente a los efectos nocivos de los avances tecnológicos, por un lado. Pero al mismo tiempo, ayudarse, acompañarse y adelantarse mediante los recursos más avanzados de la tecnología de la información y comunicación para asegurar estándares de trabajo decente, es decir, de cumplimiento con los derechos humanos laborales” (Arese, 2020, p. 73).

⁶ Cf. Proyecto de Carta de Derechos Humanos Emergentes. IDHC, Barcelona, Págs. 2-3. El documento está disponible en: <https://catedraunescodh.unam.mx/catedra/catedradh2007/SeminariosCatedra/Documentos/CartaDerechosEmergentesDH.pdf>

⁷ Observación General N.º 25 (2020) del Comité de Derechos Económicos, Sociales y Culturales, párr. 16, Naciones Unidas, documento E/C.12/GC/25.

4. Del trabajo decente al trabajo emergente: transformación del paradigma laboral

El concepto de trabajo decente, promovido por la OIT como eje de su programa de acción, representó un avance decisivo en la humanización del trabajo. No obstante, las transformaciones tecnológicas y la expansión de la economía digital han dado lugar a nuevas formas de empleo –teletrabajo, plataformas digitales, trabajo automatizado y subordinación algorítmica– que han reconfigurado el vínculo laboral clásico.

En esta línea, como observa Rázuri Vargas (2023, p. 64), “el Derecho Laboral siempre ha respondido a la coyuntura a la que se enfrenta, lo cual significa que éste es una creación del contexto mundial, lo que implica que siempre estará en constante cambio, no pudiendo utilizar las mismas respuestas de manera transversal a todas las épocas indistintamente”.

Estas modalidades, agrupadas bajo la noción de trabajo emergente, se caracterizan por la flexibilidad, la deslocalización y la mediación tecnológica. Aunque amplían las posibilidades de inserción laboral, también introducen riesgos como la precarización, la ausencia de protección social, la despersonalización del empleador y la pérdida de control sobre las condiciones de trabajo.

La subordinación algorítmica –fenómeno por el cual las decisiones laborales (asignación de tareas, evaluación, sanción) son tomadas o gestionadas por sistemas automatizados de decisión– redefine el poder de dirección del empleador y plantea dilemas sobre la autonomía y la dignidad del trabajador.

Durante la fase de diseño o entrenamiento de los algoritmos pueden incorporarse variables que, aun de manera involuntaria, generen tratos diferenciales hacia determinadas categorías de trabajadores. En este sentido, la discriminación debe entenderse –según Jesús Rodríguez Zepeda, siguiendo una formulación clásica– como “una conducta culturalmente fundada, sistemática y socialmente extendida, de desprecio contra una persona o grupo de personas sobre la base de un prejuicio negativo o un estigma relacionado con una desventaja inmerecida, que tiene por efecto (intencional o no) dañar sus derechos y libertades fundamentales”.⁸

Esta concepción teórica resulta plenamente aplicable al ámbito digital, donde los sesgos algorítmicos reproducen desigualdades estructurales bajo nuevas formas, encubiertas tras la apariencia de neutralidad tecnológica. En coincidencia con esta idea, Stekelberg Poses advierte que el “avance de las nuevas tecnologías, de la robotización y de la Inteligencia Artificial plantean desafíos trascendentes en la esfera laboral a nivel mundial. En este contexto, el Derecho del Trabajo desempeña un papel crucial (...) al posicionarse como un colectivo garante de la protección y priorización del empleo humano” (Stekelberg Poses, 2023, p. 3).

Así, la IA actúa simultáneamente como instrumento de eficiencia y fuente de desigualdad, dependiendo de quién la controla y cómo se regula su uso; de allí que garantizar un acceso equitativo a la IA no sea solo una cuestión tecnológica, sino una exigencia de justicia laboral y una actualización necesaria del concepto de trabajo decente.

⁸ Citado por Calvo (2022, p. 279).

5. Nuevas desigualdades laborales y obligaciones internacionales

La brecha digital genera una nueva forma de desigualdad: una exclusión cognitiva y tecnológica que afecta la inserción, permanencia y ascenso en el empleo. Quien no accede o no domina las herramientas de IA se encuentra en desventaja frente a quienes sí pueden utilizarlas eficazmente.

El informe “Perspectivas sociales y del empleo en el mundo: tendencias 2023” de la OIT señala que “muchos expertos consideran paradójico que, a pesar de la disponibilidad y los rápidos avances de las tecnologías digitales, la productividad se ralentice”, lo que demuestra que el progreso tecnológico no garantiza por sí solo mejores condiciones sociales ni laborales. Asimismo, la OIT advierte que “las instituciones y las políticas del mercado de trabajo son esenciales no solo para potenciar el crecimiento de la productividad, sino también para asegurar una justa distribución de las ganancias de productividad una vez obtenidas” (pp. 87–88).

De ello se deriva el deber del Estado de regular, educar y garantizar la capacitación digital, especialmente en sectores vulnerables, conforme a los principios de igualdad sustantiva, no regresividad y progresividad. Hoy, ello no solo se traduce en un derecho sino en una exigencia constitucional⁹. Como indica Maldonado Smith, “nos enfrentamos a una ‘caja negra’, porque, aunque eventualmente podamos conocer cuál fue la información de entrada que se suministró al algoritmo y cuál fue su conclusión, no podemos acreditar el procedimiento específico bajo el que se llegó a esa decisión” (*op. cit.*, p. 94).¹⁰

En concordancia, la Comisión Mundial sobre el Futuro del Trabajo de la OIT propone “revitalizar el contrato social mediante la inversión en las capacidades de las personas, las instituciones del trabajo y el trabajo decente y sostenible.”¹¹

6. Conclusión

La IA se ha convertido en un eje estructural de la vida social y laboral contemporánea. Su incorporación masiva redefine no solo las formas de trabajar, sino también los parámetros de igualdad, dignidad y acceso al conocimiento.

Es importante destacar que la defensa de los derechos de los trabajadores debe partir de una base normativa clara: el reconocimiento del acceso equitativo a la IA como un derecho humano emergente. Solo a partir de esta premisa los Estados podrán adoptar medidas efectivas para regular su uso, garantizar su aplicabilidad y asegurar la igualdad de oportunidades en el ámbito laboral.

⁹ El Art. 76 de la Constitución de la Provincia de Jujuy incorporó expresamente la IA o no humana en la reforma constitucional del año 2023. Celebramos por nuestra parte la consagración legislativa que necesariamente debe traducirse en un serio compromiso del Estado provincial para concretar los mandatos constitucionales que los convencionales constituyentes han querido consagrar. No es caprichoso señalar que el reconocimiento del uso de la IA no se agota con esa declaración *stricto sensu*. Demanda más que el reconocimiento de las tecnologías y sistemas de IA que ya conviven entre nosotros, que el Estado asuma la garantía, frente a su uso, de que todo otro derecho no sea vulnerado. Este es el sentido, teleológicamente hablando, en el que, en el marco de una interpretación consecuencialista, entendemos debe interpretarse la norma constitucional.

¹⁰ Citando a Pasquale, *The Black Box Society: The Secret Algorithms that control Money and Information*, p. 34.

¹¹ OIT. *Comisión Mundial sobre el Futuro del Trabajo: Trabajar para un futuro más prometedor*. Informe, Ginebra, 2019, citado por Arese (2020, p. 67).

El tránsito del trabajo decente al trabajo emergente no debe implicar una pérdida de derechos, sino una evolución normativa que reafirme los principios de libertad, equidad y dignidad humana en un entorno digital. Para posibilitar un tránsito justo –sin afectar los derechos adquiridos ni permitir nuevas formas de discriminación en el acceso o permanencia laboral– resulta imprescindible el reconocimiento de este derecho humano emergente.

En un plano más específico, se impone la necesidad de regular los algoritmos que intervienen en los procesos laborales, en tanto potenciales factores de discriminación o generadores de sesgos. Regular no implica prohibir, sino establecer los márgenes legales, éticos y morales que aseguren un uso justo y transparente de la IA en el trabajo. Ya sea que la IA se utilice como criterio de selección –a través de algoritmos automatizados– o como herramienta indispensable para el acceso y desempeño laboral, su funcionamiento debe estar sujeto a una regulación estatal fundada en este derecho humano emergente.

Así como en algún momento fue requisito saber escribir a máquina y luego dominar programas de ofimática¹², hoy parece avizorarse una nueva exigencia: el manejo de la IA como competencia básica para la inclusión laboral. Quien no accede o no domina estas herramientas enfrenta una desventaja estructural, que puede traducirse en actos de discriminación y exclusión tecnológica.

En varias provincias argentinas, incluida la nuestra (Jujuy), persisten brechas significativas de conectividad en zonas rurales y periurbanas, altos índices de informalidad laboral y una insuficiente capacitación digital. Estas condiciones agravan el riesgo de exclusión tecnológica y profundizan la desigualdad en el acceso a las oportunidades laborales mediadas por IA. Ello refuerza la necesidad de políticas públicas diferenciadas que garanticen un acceso equitativo y efectivo a las nuevas tecnologías.

La ética debe mantener presencia permanente para regular, limitar y evitar excesos innecesarios que puedan dañar a la humanidad; la IA no debe desplazar al trabajo humano, sino complementarlo. Como opina Maldonado Smith, “la ecuación expresada habría de brindar supremacía a la tutela de la igualdad, por lo que el desarrollo tecnológico sin frenos y su aplicación al ámbito laboral-empresarial únicamente podría permitirse en tanto fuere coherente con la tutela de los derechos fundamentales” (*op. cit.*, p. 79).

Negar o restringir este acceso significaría permitir una nueva forma de exclusión, no ya basada en la propiedad de los medios de producción, sino en el acceso desigual al conocimiento y la tecnología. El desafío, entonces, es construir un marco jurídico internacional capaz de garantizar que el progreso tecnológico no erosione la humanidad del trabajo, sino que la expanda. Como advierte Luis Camacho, “la omnipresencia de la disrupción digital y los nuevos procesos laborales está constantemente modificando y reajustando el panorama laboral, desafiando el sistema clásico de relaciones laborales y generando cambios significativos” (Camacho, 2024, p. 2).

¹² La ofimática es el uso de herramientas informáticas para automatizar y optimizar las tareas de oficina, como la creación de documentos, la gestión de hojas de cálculo y la comunicación.

En definitiva, el acceso equitativo a la IA se configura como un derecho humano emergente necesario para equilibrar ese proceso y evitar que el cambio tecnológico erosione la justicia social. ¿Podrá el Derecho, en su dimensión convencional y social, acompañar el ritmo del cambio tecnológico sin abdicar de su núcleo humanista?

Mientras el derecho positivo avanza hacia el reconocimiento del acceso equitativo a la IA como derecho humano emergente, la interpretación dinámica tridimensional se proyecta como una herramienta idónea para acompañar esta transición, preservando la eficacia práctica de los derechos laborales en un entorno digital en constante transformación.

Referencias

- Arese, C. (2020). *Trabajo decente y derechos humanos laborales en la era digital*. Revista Iberoamericana de Derecho del Trabajo y de la Seguridad Social.
- Calvó, Leonardo S., *Cálculo de indemnizaciones laborales*, 1ra Ed., San Salvador de Jujuy, El Fuste, 2022.
- Camacho, Luis (2024). “Noticias del cielo: reflexiones sobre la tecnología y el humanismo contemporáneo”, *Revista Cielo*, n.º 11.
- Carril, M. P., & Calvó, L. S. (2025, 14 julio). “Violencia digital e IA generativa: el fallo «UndressHer.app» como punto de inflexión en materia de tutela judicial”, *Microjuris Argentina* (MJ-DOC-18329-AR).
- Comité de Derechos Económicos, Sociales y Culturales de las Naciones Unidas (2020). *Observación general N.º 25: La ciencia y los derechos económicos, sociales y culturales (artículo 15.1 b, c y 15.3 del Pacto)*. Doc. E/C.12/GC/25.
- Corte Interamericana de Derechos Humanos (2017). *Caso Lagos del Campo vs. Perú (Fondo, Reparaciones y Costas)*, Sentencia de 31 de agosto de 2017, Serie C No. 340.
- Instituto de Democracia y Derechos Humanos de la Pontificia Universidad Católica del Perú (IDEHPUCP). (2023). *Nuevas tecnologías y derechos humanos: Análisis sobre escenarios de posibles amenazas* (Informe de Investigación N.º 7). Lima: PUCP.
- Institut de Drets Humans de Catalunya (IDHC). Proyecto de Carta de Derechos Humanos Emergentes. Barcelona, IDHC.
- Kurczyn Villalobos, P. (2023). *Trabajo y derechos humanos en la era de la inteligencia artificial*. Ciudad de México: Universidad Nacional Autónoma de México.
- Maldonado Smith, M. (2021). “Algoritmos y derechos fundamentales: entre la opacidad y la responsabilidad”, *Revista Chilena de Derecho y Tecnología*, 10(2), 71–99.
- Organización Internacional del Trabajo (OIT). (2023). *Perspectivas sociales y del empleo en el mundo: Tendencias 2023*. Ginebra: Oficina Internacional del Trabajo.
- Organización Internacional del Trabajo (OIT). (1999). *Memoria del Director General: Trabajo decente*. Conferencia Internacional del Trabajo, 87.ª reunión, Ginebra.
- Pontificia Universidad Católica del Perú (PUCP). (2023). *Inteligencia artificial y derechos laborales: riesgos y desafíos regulatorios*. Lima: PUCP.
- Rázuri Vargas, C. A. (2023). “¿Avanzamos hacia un trabajo decente? La inteligencia artificial como herramienta de mejora para el impulso del empleo decente”, *Revista Laborem*, n.º 28, 50-70, Lima.
- Salinas Atencio, Milagros A. y Guzmán Napurí, Christian, “La inteligencia artificial, los sesgos del algoritmo y la discriminación en las relaciones laborales”, *Revista Laborem*, n.º 31 (2025).

Stekelberg Poses, L. (2023). “El trabajo emergente y la subordinación algorítmica”, *Revista Iberoamericana de Derecho Laboral*, (9), 33–59.


EL BENEFICIO DE LITIGAR SIN GASTOS COMO INSTRUMENTO DE ACCESO A LA JUSTICIA

The Benefit of Litigating Without Costs as a Tool for Access to Justice

Henoch Romero Boue*

Universidad Nacional del Comahue

henochromeroboue@gmail.com

 <https://orcid.org/0009-0003-4255-8985>

RECIBIDO 14/11/2025 - ACEPTADO 17/11/2025

Resumen

El Beneficio de Litigar sin Gastos (BLSG) es una garantía esencial para el acceso a la justicia frente a la desigualdad económica. El artículo analiza sus bases constitucionales y convencionales, con foco en el régimen del Código Procesal de Río Negro (Ley 5.777) y la competencia de los Juzgados de Paz. Examina los criterios de otorgamiento, las tensiones interpretativas y el tratamiento de las personas jurídicas. Ante el esquema actual de verificación manual, propone una reforma de gestión y tecnología basada en la interoperabilidad de datos. Se sostiene que el BLSG debe entenderse como una política pública de inclusión y democratización judicial en clave digital.

Palabras clave:

acceso a la justicia, digitalización judicial, igualdad, Justicia de Paz, interoperabilidad.

Abstract

The Benefit of Litigating Without Costs (BLSG) is an essential safeguard for ensuring access to justice in the face of economic inequality. This article analyzes its constitutional and conventional foundations, focusing on the procedural regime of Río Negro's Code of Procedure (Law 5,777) and the jurisdiction of Peace Courts. It examines the criteria for granting the benefit, interpretive tensions, and the treatment of legal entities. Given the current system of manual verification, the article proposes a management and technological reform based on data interoperability. It argues that the BLSG should be understood as a public policy of judicial inclusion and democratization in the digital era.

Keywords:

access to justice, judicial digitalization, equality, Peace Courts, interoperability.

1. Introducción

El acceso a la justicia constituye un derecho humano fundamental y una condición esencial del Estado de Derecho. No basta con reconocer formalmente la posibilidad de acudir a los tribunales: resulta indispensable garantizar que ninguna persona quede excluida del proceso por razones económicas, una barrera especialmente crítica en contextos de crisis recurrentes como los que atraviesa la Argentina. Ello impone al Estado el deber positivo de garantizar vías efectivas de tutela judicial y eliminar los obstáculos económicos que la restrinjan.

* Abogado, Universidad Nacional del Comahue. Especialista en Derecho Procesal Civil, Universidad de Buenos Aires. Especialista en Justicia Constitucional y Derechos Humanos (Universidad de Bolonia).

En este marco, el beneficio de litigar sin gastos (BLSG) se erige como una herramienta clave para efectivizar el acceso real a la justicia. Permite que quienes carecen de recursos económicos puedan litigar sin abonar tasas judiciales, honorarios profesionales, pericias ni costas, haciendo operativa la garantía de tutela judicial efectiva.

Sin embargo, el instituto presenta desafíos interpretativos y prácticos de gran relevancia. Su aplicación exige ponderar –con prudencia judicial– la tensión entre la protección del derecho de quien no puede afrontar los costos del proceso y la necesidad de evitar abusos que afecten los intereses de la contraparte o del Estado, que soporta el costo de la administración de justicia. La cuestión adquiere particular complejidad cuando se trata de personas jurídicas con fines de lucro, o cuando el tribunal debe decidir entre una concesión total o parcial del beneficio, valorando las consecuencias económicas y sistémicas de su resolución.

En la Provincia de Río Negro, emerge el nuevo Código Procesal Civil y Comercial (Ley N° 5.777) introduciendo un cambio significativo al trasladar la competencia en materia de BLSG a los Juzgados de Paz, redefiniendo su rol institucional y planteando interrogantes sobre la uniformidad de criterios y los mecanismos recursivos. Este rediseño normativo constituye un ejemplo ilustrativo de un proceso más amplio de descentralización judicial que se advierte en el ámbito provincial argentino.

El presente trabajo propone una lectura integral del BLSG como instrumento de acceso a la justicia y garantía de equidad, incorporando el análisis de los factores económicos y de los intereses en conflicto que condicionan su aplicación práctica. Asimismo, se examina la experiencia rionegrina en el marco de las tendencias contemporáneas de las políticas públicas de acceso a la justicia, donde la dimensión tecnológica y la gestión eficiente cobran creciente protagonismo. En este sentido, se sostiene que la efectividad del BLSG en la práctica procesal contemporánea no depende solo de normas claras, sino también de mecanismos administrativos y herramientas tecnológicas que garanticen transparencia, celeridad y racionalidad en su otorgamiento, sin menoscabar las salvaguardas procesales. En definitiva, se propone avanzar hacia un rediseño integral del instituto como política pública, que combine igualdad sustancial, racionalidad económica y transformación digital del sistema judicial.

2. Fundamento constitucional y convencional del instituto

El Beneficio de Litigar Sin Gastos (BLSG) encuentra su sustento primario en los artículos 16 (igualdad) y 18 (garantía de defensa en juicio) de la Constitución Nacional, y se integra y robustece con los instrumentos internacionales de derechos humanos con jerarquía constitucional (art. 75 inc. 22 CN), en particular, los arts. 8 (Garantías Judiciales) y 25 (Protección Judicial) de la Convención Americana sobre Derechos Humanos (CADH). La Corte Suprema de Justicia de la Nación ha reconocido reiteradamente que el acceso a la justicia forma parte del contenido esencial de los derechos humanos y no puede depender de la capacidad económica del litigante, sentando precedentes clave:

- En “Kot c/ Universidad de Buenos Aires” (Fallos 241:291) sostuvo que las tasas judiciales no deben erigirse en un obstáculo para el ejercicio del derecho de defensa.
- En “Q.C., S.Y. c/ Gobierno de la Ciudad de Buenos Aires” (Fallos 335:452) vinculó el acceso a la justicia con la protección de los derechos sociales y la igualdad real.
- En “A.,M.A. c/ Estado Nacional” (Fallos 329:5266) reafirmó que el acceso efectivo a la jurisdicción no puede depender de la capacidad económica del litigante.

A nivel convencional, el Sistema Interamericano de Derechos Humanos prohíbe la discriminación basada en la posición económica. La Corte IDH ha establecido que los Estados tienen el deber positivo de remover los obstáculos económicos que impidan el disfrute pleno de los derechos, especialmente en contextos de vulnerabilidad. En la Opinión Consultiva OC-11/90 y en el Caso “Cantos vs. Argentina” (2005), la Corte determinó que la imposición de costas y gastos judiciales desproporcionados, o la falta de asistencia legal gratuita, puede configurar una violación de la protección judicial efectiva (art. 25 CADH) y una discriminación por motivos económicos.

En este marco, el BLSG no constituye una excepción ni una concesión graciosa, sino una manifestación concreta del principio de igualdad sustancial orientada a garantizar la eficacia real del derecho de acción. Asegura que el acceso a la jurisdicción no se vea frustrado por la carencia de medios económicos, garantizando así la prestación de justicia sin distinción entre las partes por dicha circunstancia. Como explica Díaz Solimine (2003), en sus dos sentidos interrelacionados, uno “funcional” para que objetivamente funcione el servicio de justicia, y otro “personal” como auxilio para el justiciable.

3. Concesión total o parcial del beneficio: ponderación de intereses y problema económico

En el ámbito de la provincia de Río Negro, el BLSG se encuentra incorporado en el nuevo Código Procesal Civil y Comercial aprobado por la Ley 5.777 (diciembre de 2024), entre los artículos 72 a 81. El artículo 81 dispone que el beneficio puede otorgarse en forma total o parcial. Sin embargo, al no especificar dicha norma en qué consiste concretamente esa parcialidad –porcentajes, etapas procesales o tipos de gastos comprendidos–, deja un margen interpretativo que la jurisprudencia provincial ha debido integrar.

En la práctica judicial rionegrina, se ha consolidado una línea que entiende que, cuando no se acredita una total carencia económica pero sí una dificultad relevante para afrontar los gastos iniciales del proceso, corresponde conceder el beneficio parcialmente, limitándose a la exención de tasas, sellados y contribuciones. Así, se libera al solicitante de los gastos necesarios para iniciar la demanda, sin extender el beneficio al resto emergente del proceso ante una eventual imposición de eventuales gastos, costas y honorarios casuísticos.

Esta interpretación se apoya en una lectura prudente del mismo precepto citado, que reconoce la facultad judicial de graduar el alcance del beneficio sin autorizar una concesión total automática ante toda alegación de insuficiencia. Desde esta perspectiva, la concesión parcial no responde a un criterio meramente cuantitativo, sino a una decisión responsable de política judicial con impacto económico directo. Una concesión total implica trasladar

al Estado o a la contraparte el costo íntegro del litigio, lo cual exige un juicio riguroso sobre la real imposibilidad económica del solicitante. En cambio, la concesión parcial —aún limitada— procura garantizar el acceso a la jurisdicción sin desnaturalizar la función del instituto ni comprometer irrazonablemente los recursos públicos.

El análisis de procedencia, entonces, debe equilibrar tres intereses básicos concurrentes:

- 1) *El del solicitante*: vinculado al derecho de acceso efectivo a la justicia, que exige remover los obstáculos económicos que impidan su participación en el proceso.
- 2) *El de la contraparte*: que no debe verse compelida a litigar contra quien no asume costo alguno, evitando así el riesgo de litigios temerarios o abusivos.
- 3) *El del erario público*: que impone racionalidad en el uso de los recursos estatales y preserva la integridad del instituto para los casos de auténtica necesidad.

Este equilibrio tripartito exige un examen casuístico y fundado, donde la “insuficiencia de recursos” no se mida con una visión contable rígida, sino desde la realidad económica integral del solicitante. Ello obliga al tribunal a valorar la prueba con razonabilidad y a dictar una resolución que armonice tutela judicial efectiva y sostenibilidad del sistema, evitando tanto la denegación arbitraria como la concesión irreflexiva.

Cabe agregar que la insuficiencia no se reduce a la mera ausencia de ingresos, sino que exige valorar la liquidez efectiva del solicitante. Efectivamente, una persona puede tener bienes registrables o un patrimonio inmovilizado que, sin embargo, no le permita afrontar los gastos del proceso sin afectar su subsistencia o el normal desarrollo de su actividad. Este criterio —centrado en la disponibilidad real de recursos— otorga sentido al beneficio y preserva su carácter excepcional, evitando tanto su abuso como la denegación irrazonable del acceso a la jurisdicción.

En esa línea, es dable afirmar que la concesión total del BLSG presenta una mayor complejidad decisoria para quien juzga, en tanto supone eximir al solicitante de todas las cargas económicas derivadas del proceso, desde su inicio hasta su conclusión. Tal amplitud exige una verificación exhaustiva y un estándar probatorio más riguroso, ya que la exención plena impacta tanto en la posición de la contraparte —que se ve privada de enfrentar un litigio en condiciones de igualdad económica— como en la administración de justicia, que asume indirectamente los costos del litigio.

Por ello, el beneficio total debe reservarse a los casos de carencia comprobada de capacidad económica y recursos líquidos, donde el solicitante se encuentre materialmente imposibilitado de afrontar los gastos sin comprometer su subsistencia. En cambio, cuando se verifica una insuficiencia relativa o transitoria, corresponde una concesión limitada o ajustada, que permita remover los obstáculos de acceso a la jurisdicción sin desnaturalizar el carácter excepcional del instituto. Este enfoque preserva el equilibrio entre la tutela judicial efectiva y la razonabilidad en el uso de los recursos, evitando tanto la denegación arbitraria como la extensión indiscriminada del beneficio.

4. Personas jurídicas solicitantes: control reforzado y razonabilidad probatoria

La situación de las personas jurídicas que solicitan el BLSG presenta particularidades que exigen un control más cuidadoso y razonado. A diferencia de las personas físicas, su análisis no puede limitarse a la mera acreditación de carencia económica, sino que requiere una evaluación integral de su clase, objeto social, grado de actividad, capacidad operativa y situación fiscal, conforme los elementos efectivamente aportados en juicio.

El Tribunal debe ponderar, en cada caso, si se trata de una asociación civil sin fines de lucro, una fundación, una cooperativa inactiva, una sociedad comercial con actividad reducida o una empresa con fines de lucro plenamente operativa. Este examen permite determinar si la alegada falta de recursos es genuina o encubre una estrategia procesal dilatoria o evasiva. En la provincia de Río Negro, el Superior Tribunal de Justicia de Río Negro ha sostenido reiteradamente un criterio restrictivo para las personas jurídicas con fines de lucro:

“Cuando la que demanda es una sociedad comercial que se inspira en fines de lucro, el instituto debe ser apreciado con prudencia, a fin de no desnaturalizarlo” (STJRN, Turbine Power Co. S.A., Se. 13/2009).

“La sola condición de tratarse de una persona ideal con fines de lucro no habilita la denegación del beneficio, pero la prudencia exige un análisis meduloso de su situación patrimonial y de la imposibilidad fáctica de hacerse de recursos” (STJRN, Vicente Robles S.A., Se. 107/2014).

En este marco, la exigencia probatoria debe guardar proporción y sentido práctico. No resulta razonable requerir balances contables cuando la entidad acredita inactividad fiscal o ausencia total de operaciones registradas, pues ello tornaría el pedido probatorio impracticable y ajeno a la finalidad del instituto. Lo relevante es verificar la capacidad económica efectiva o liquidez, entendida como la posibilidad concreta de hacer frente a los costos del proceso sin comprometer la subsistencia o el funcionamiento institucional.

El principio dispositivo, que impone a las partes la carga de aportar la prueba, debe armonizarse con el deber judicial de dictar una sentencia ajustada a la realidad económica del caso. Ello autoriza al magistrado, cuando la prueba resulte insuficiente o confusa, a disponer medidas para mejor proveer, sin sustituir la carga probatoria del solicitante, sino complementando la información necesaria para una decisión fundada. De este modo, el control judicial sobre las personas jurídicas debe combinar rigor técnico con razonabilidad práctica, ponderando su naturaleza, objeto y grado de actividad. Solo así puede garantizarse que la exigencia probatoria no frustre la finalidad garantista del beneficio ni desvirtúe el principio de acceso efectivo a la justicia.

En definitiva, el examen sobre la procedencia del beneficio en personas jurídicas debe orientarse a verificar su liquidez efectiva y capacidad económica real, evitando requerimientos formales carentes de sentido práctico cuando la entidad se encuentra inactiva o sin operaciones registradas.

5. Competencia exclusiva de los Juzgados de Paz en Río Negro

El nuevo Código Procesal Civil y Comercial de Río Negro (Ley 5.777) introdujo una modificación relevante al otorgar competencia exclusiva a los Juzgados de Paz para conocer en

los procesos de BLSG (art. 5, inc. 11). Esta decisión normativa responde, según se observa, a una política de descentralización judicial y acercamiento territorial, en línea con el principio de tutela judicial efectiva.

Desde el punto de vista funcional, esta reasignación de competencia representa tanto una oportunidad como un desafío. Por un lado, acerca la justicia al ciudadano y permite un tratamiento más inmediato y contextualizado de las situaciones de vulnerabilidad económica. Por otro, incrementa la carga operativa sobre organismos ya saturados y obliga a reforzar sus capacidades técnicas, humanas y tecnológicas. Entre las principales dificultades prácticas pueden mencionarse:

- 1) Sobrecarga funcional, debido a la multiplicidad de materias a cargo de los Juzgados de Paz.
- 2) Falta de uniformidad en los criterios probatorios y en el alcance del beneficio, derivada de la dispersión territorial.
- 3) Necesidad de capacitación específica, en particular para valorar adecuadamente la prueba contable y económica.

Sobre este punto, cabe destacar que en el precedente “Chaves, Melina Estefanía s/ Beneficio de litigar sin gastos” (STJRN, Se. 21/2025), el Superior Tribunal de Justicia de Río Negro estableció que la competencia para entender en las solicitudes del BLSG corresponde al Juzgado de Paz de la Circunscripción Judicial donde tramita el proceso principal, aun cuando la petición se hubiera iniciado en otro ejido. Este criterio garantiza coherencia jurisdiccional y proximidad territorial en el acceso a la justicia. Así, por ejemplo, si una persona sufre un accidente de tránsito en una localidad con Justicia de Paz, deberá tramitar allí el beneficio, aunque la causa principal se sustancie en otra localidad dentro de la misma Circunscripción, manteniéndose de ese modo la unidad jurisdiccional.

La experiencia demuestra que la justicia de proximidad puede ser un medio eficaz para garantizar accesibilidad, siempre que esté acompañada por inversión institucional y herramientas tecnológicas adecuadas. De lo contrario, el propósito de equidad se ve neutralizado por la sobrecarga y la demora estructural.

En este marco, la reasignación de nuevas competencias no sólo tiene significancias procesales, sino también socioeconómicas, pues implica reconocer que el acceso a la justicia no puede depender de la distancia geográfica ni de la disponibilidad de recursos tecnológicos o profesionales en cada localidad. De allí que la política judicial deba acompañarse de inversiones sostenidas en infraestructura y conectividad, como condición indispensable para la equidad territorial.

6. Propuesta de criterios orientadores para una aplicación uniforme del beneficio

La práctica judicial evidencia que la aplicación del BLSG carece de pautas uniformes en aspectos esenciales como la concesión parcial, la valoración de la prueba o la suficiencia económica. Para superar la dispersión interpretativa y garantizar decisiones equitativas, se proponen los siguientes criterios orientadores:

- 1) *Criterio de amplitud con razonabilidad*: interpretar el beneficio en forma amplia para garantizar el acceso a la justicia, pero exigiendo convicción fundada sobre la real insuficiencia económica.
- 2) *Graduación del beneficio*: justificar expresamente las razones de una concesión total o parcial, aplicando la exención limitada (tasas y sellados) cuando la dificultad no sea absoluta.
- 3) *Carga probatoria diferenciada y control de liquidez*: exigir documentación contable o fiscal solo cuando sea razonablemente esperable que la entidad la posea; de lo contrario, priorizar la acreditación de inactividad o liquidez efectiva, entendida como la capacidad real de afrontar los costos inmediatos del proceso.
- 4) *Medidas para mejor proveer*: habilitar su uso cuando la prueba sea insuficiente, evitando denegaciones formales que frustren el derecho de acción.
- 5) *Motivación cualitativa*: fundamentar la decisión en el valor demostrativo de la prueba, no en la cantidad de documentos acompañados.
- 6) *Perspectiva económica y social*: concebir el beneficio como instrumento de justicia material y política pública, no como dispensa graciosa, equilibrando tutela judicial y sostenibilidad del gasto público.

7. La interoperabilidad digital y el control de insuficiencia: evolución de la prueba informativa (de *lege ferenda*)

El análisis de procedencia del BLSG exige una valoración casuística y rigurosa de la insuficiencia económica del solicitante. Sin embargo, el control de tal extremo mediante los mecanismos tradicionales de prueba informativa —esto es, el libramiento de oficios a organismos públicos y privados— se presenta hoy como un procedimiento lento, fragmentado y burocrático. En la práctica judicial, la obtención de respuestas de organismos tales como ANSES, AFIP, registros de propiedad, agencias de rentas, o entidades financieras, entre muchos otros posibles, suele demorar varias semanas o incluso meses, lo que conspira directamente contra la finalidad del beneficio y el principio de celeridad procesal que debe regirlo.

Si bien se han implementado avances interjurisdiccionales mediante herramientas como el “Bus Federal de Oficios Judiciales”¹ o las plataformas electrónicas de notificación, estos sistemas representan pasos iniciales hacia la interoperabilidad, aunque todavía funcionan principalmente como canales de gestión documental y no como verdaderas redes de intercambio de datos. La diferencia no es menor: mientras el primero digitaliza un trámite manual, el segundo permitiría la conexión directa y segura entre bases de datos públicas, posibilitando al tribunal acceder y certificar en tiempo real la información relevante sobre la situación fiscal, patrimonial y laboral del solicitante, con pleno respeto por las garantías constitucionales.

En este sentido, la propuesta de incorporar mecanismos de interoperabilidad digital en la verificación patrimonial del BLSG debería pensarse bajo una doble clave: por un lado, como una forma de auxilio probatorio al juez, que garantice una constatación más precisa, objetiva y ágil de la insuficiencia de medios; y por otro, como una actualización tecnológica

¹ Cf. <https://www.bus-justicia.org.ar/index.php/bus-federal/guias-tramite>.

necesaria para adecuar el proceso judicial a la realidad contemporánea, en la que la información económica y fiscal se encuentra registrada en entornos digitales interconectados.

Desde luego, esta evolución debe armonizarse con los principios de protección de datos personales previstos en la Ley 25.326 y su decreto reglamentario, garantizando que la interoperabilidad opere bajo estándares de confidencialidad, consentimiento y finalidad legítima. El acceso judicial a dicha información debe ser acotado al objeto del proceso y sujetarse a los principios de proporcionalidad y necesidad.

En definitiva, la interoperabilidad digital –entendida como un sistema integral de consulta de datos entre organismos públicos y judiciales– se erige como una herramienta indispensable para compatibilizar los fines protectores del BLSG con las exigencias de un proceso eficiente y transparente. Su implementación, en tanto medida *lege ferenda*, no sólo fortalecería la tutela judicial efectiva, sino que además respondería a la necesidad de adecuar la administración de justicia a las condiciones tecnológicas y socioeconómicas actuales, donde la verificación manual resulta obsoleta e ineficiente. De manera similar, esa opción resulta viable desde la perspectiva de agilizar la tramitación del procedimiento de BLSG, reforzando, a su vez, la transparencia institucional y la confianza ciudadana en el sistema judicial.

8. Conclusiones: la tutela efectiva y el imperativo de la innovación digital

El BLSG trasciende la mera dispensa procesal; constituye una manifestación irrenunciable del compromiso judicial con la igualdad sustancial y la garantía de acceso a la justicia. Este trabajo ha examinado cómo la fuente constitucional y convencional compromete a los Estados a remover activamente las barreras económicas, exigiendo a los tribunales un examen riguroso, prudente y fundado con los alcances de concesión que correspondan según el caso.

La experiencia particular de Río Negro, con la descentralización de la competencia a los Juzgados de Paz, es en cierta forma ejemplificadora de los esfuerzos por acercar la justicia a la población. Sin embargo, este modelo de proximidad obliga a reforzar esos organismos donde cada vez más se les incorporan otras tareas o procesos de índole procesal-jurídico.

De manera similar, en el actual contexto, la interoperabilidad de datos –planteada como la reforma *lege ferenda*– emerge como el imperativo de gestión para la materialización de la tutela judicial efectiva. El camino es reemplazar la ineficiencia de los oficios por un sistema de consulta automatizada que, sin suplir la carga probatoria del solicitante, actúe como un auxiliar judicial ágil y fehaciente para la verificación de los extremos patrimoniales.

La efectividad futura del BLSG dependerá, en última instancia, de una convicción judicial garantista acompañada por una voluntad política sostenida de modernización institucional. Solo mediante el liderazgo de los máximos tribunales, la coordinación entre los poderes públicos, las colegiaturas profesionales y los organismos fiscales, junto con un respaldo normativo que habilite la interoperabilidad digital, podrá asegurarse que las decisiones sobre la insuficiencia de recursos se funden en datos objetivos, precisos y oportunos.

En los últimos años, la interoperabilidad digital ha comenzado a consolidarse como una política pública judicial orientada a optimizar la gestión de causas y fortalecer el acceso a la justicia. En este sentido, la Junta Federal de Cortes y Superiores Tribunales de Justicia (JUFEJUS) y el Ministerio de Justicia y Derechos Humanos de la Nación suscribieron en 2021 un convenio para la implementación de la plataforma “Bus Justicia”, destinada a permitir el intercambio seguro y trazable de expedientes, documentos y servicios electrónicos entre los poderes judiciales provinciales y distintos organismos públicos y privados². Este desarrollo constituye un paso decisivo hacia la interoperabilidad judicial como herramienta de integración sistémica y eficiencia administrativa.

En diciembre de 2024, la Corte Suprema de Justicia de la Nación anunció su incorporación al Bus Federal de Justicia, confirmando así la viabilidad operativa del sistema y la orientación institucional hacia un modelo de justicia digital coordinada (CSJN, 2024)³. Estas experiencias demuestran que la interoperabilidad no es una utopía tecnológica, sino una política posible que puede –si se articula con criterios garantistas– dotar de objetividad, transparencia y celeridad a decisiones sensibles como la evaluación de la insuficiencia de recursos en el otorgamiento del beneficio.

En síntesis, la evolución del BLSG exige superar el modelo probatorio artesanal mediante soluciones tecnológicas interoperables que preserven la garantía judicial y la verificación razonable de la insuficiencia de recursos. El acceso a la justicia no se asegura solo con normas, sino con gestión pública inteligente y con sobre todo magistrados comprometidos en convertir los principios constitucionales en prácticas judiciales efectivas. El desafío, en definitiva, no es solo garantizar el acceso a la justicia, sino construir una justicia accesible, inteligente y tecnológicamente inclusiva.

Referencias

- Corte Suprema de Justicia de la Nación, “Kot c/ Universidad de Buenos Aires”, (Fallos 241:291), 1957.
- Corte Suprema de Justicia de la Nación, “Q.C., S.Y. c/ GCBA”, (Fallos 335:452), 2012.
- Corte Suprema de Justicia de la Nación, “A., M.A. c/ Estado Nacional”, (Fallos 329:5266), 2006.
- Código Procesal Civil y Comercial de la provincia de Río Negro. Ley 5.777. Año 2024.
- Díaz Solimine, O. L. (2003). El beneficio de litigar sin gasto. (2ª ed.). Buenos Aires: Hammurabi.
- Corte IDH (1990). “Excepciones al agotamiento de los recursos internos (arts. 46.1, 46.2.a y 46.2.b Convención Americana sobre Derechos Humanos)” [Opinión Consultiva OC-11/90].
- Corte IDH (2005). “Cantos vs. Argentina. Fondo, Reparaciones y Costas”. Sentencia Serie C No. 130.
- Superior Tribunal de Justicia de Río Negro (2009). “Turbine Power Co. SA s/ Beneficio de litigar sin gasto s/ Apelación”. Sentencia 13.
- Superior Tribunal de Justicia de Río Negro (2014). “Vicente Robles SA M.C.I.C.I.F. c/ Provincia de Río Negro y otra Administración de Parques Nacionales s/ Beneficio de litigar sin gastos s/ Apelación”. Sentencia 107.

² Para el anuncio del convenio, consúltase JUFEJUS (2021).

³ Este año la Corte lanzó el portal Justicia.ar: <https://www.justicia.ar/>.

Superior Tribunal de Justicia de Río Negro (2025). “Chaves, Melina Estefanía s/ Beneficio de litigar sin gastos”. Sentencia 21.

Corte Suprema de Justicia de la Nación. (2024, diciembre). La Corte Suprema se incorporó al Bus Federal de Justicia. Recuperado de <https://www.csjn.gov.ar/novedades/detalle/9189>

Junta Federal de Cortes y Superiores Tribunales de Justicia de las Provincias Argentinas (JUFEJUS). (2021, octubre). Poderes judiciales de la Argentina contarán con una plataforma digital para la interoperabilidad entre los tribunales. Recuperado de <https://www.jufejus.org.ar/poderes-judiciales-de-la-argentina-contaran-con-una-plataforma-digital-para-la-interoperabilidad-entre-los-tribunales/>

PROPIEDAD INTELECTUAL Y ENSEÑANZA DEL DERECHO DE MARCAS: EL MÉTODO DE CASO Y LA PRÁCTICA PROFESIONAL EN EL NOA

Intellectual Property and Trademark Law Teaching: The Case Method and Professional Practice in Northwestern Argentina (NOA)

Eloísa N. Casado*

Universidad Nacional de Tucumán

eloisa.casado@outlook.es

RECIBIDO 24/10/2025 - ACEPTADO 17/11/2025

Resumen

El trabajo examina la enseñanza del Derecho de Propiedad Intelectual –en particular, del régimen de marcas, desde un enfoque pedagógico práctico orientado al Noroeste Argentino. A través del método del caso y recursos digitales, propone fortalecer la formación profesional, descentralizar la práctica jurídica y favorecer un mercado más equitativo. Integra aportes pedagógicos de Camilloni, Lucarelli y enfoques de evaluación deliberativa. Se presenta el caso “Cervecería La Fulanita” como experiencia que vincula teoría jurídica, innovación didáctica y compromiso territorial.

Palabras clave:

propiedad intelectual, marcas, enseñanza jurídica, método del caso, innovación pedagógica, evaluación formativa, NOA.

Abstract

This article examines the teaching of Intellectual Property Law –particularly trademark law– from a practical, regional perspective focused on Northwestern Argentina. Using the case method and digital tools, it seeks to strengthen professional training, decentralize legal practice, and promote a more equitable market. It incorporates pedagogical contributions from Camilloni, Lucarelli, and deliberative assessment approaches. The case study “Cervecería La Fulanita” is presented as an experience that connects legal theory, educational innovation, and territorial engagement.

Keywords:

intellectual property, trademarks, legal education, case method, pedagogical innovation, formative assessment, Northwestern Argentina.

1. Introducción

A una década de la entrada en vigencia del Código Civil y Comercial de la Nación, se impone reflexionar sobre cómo la enseñanza del Derecho debe adaptarse a las transformaciones del mundo profesional y digital. Si bien el Código no regula la propiedad industrial, ésta se rige por la Ley 22.362 de Marcas y Designaciones, la Ley 24.481 de Patentes y sus normas complementarias; el nuevo paradigma unificador del Derecho privado influyó en la

* Abogada (Universidad Nacional de Tucumán). Especialista en Docencia Superior (Universidad Nacional de Jujuy). Docente especializada en derecho comercial y corporativo.

forma de comprender la función de los bienes inmateriales y de la innovación en el tráfico económico.

En la actualidad, comprender el régimen de las marcas se vuelve una competencia profesional esencial. Las marcas representan no solo un signo jurídico, sino un activo económico, cultural y simbólico que refleja la identidad de empresas y emprendedores. En provincias del Noroeste Argentino (NOA), donde las economías regionales cobran protagonismo, enseñar Propiedad Intelectual con un enfoque práctico y territorial adquiere una relevancia estratégica.

Durante años, los trámites de marcas se gestionaban exclusivamente en Buenos Aires. Sin embargo, la digitalización del Instituto Nacional de la Propiedad Industrial (INPI) transformó este panorama: hoy, abogados del NOA pueden realizar todos los trámites en línea. Esta apertura tecnológica crea oportunidades, pero también demanda una enseñanza actualizada, que forme abogados capaces de actuar en entornos digitales y de comprender la dinámica de los derechos industriales con responsabilidad ética y técnica.

En este contexto, el presente trabajo propone una experiencia de enseñanza basada en el método del caso –una estrategia que sitúa al estudiante ante un conflicto real o simulado, promoviendo análisis, argumentación y toma de decisiones–. A través del caso docente “Cervecería La Fulanita”, se busca mostrar cómo el Derecho de Marcas puede enseñarse desde la práctica, integrando teoría, tecnología y reflexión ética.

La propuesta se inscribe dentro de una línea de innovación pedagógica universitaria, apoyada en los fundamentos de la Didáctica General y Didáctica Específica (Camilloni, 2007). En esta visión, enseñar no se reduce a transmitir normas, sino a crear condiciones para pensar jurídicamente, construir identidad profesional y vincular el aula con el ejercicio real de la abogacía.

2. La enseñanza práctica de la propiedad intelectual y la formación profesional en el NOA

Enseñar Propiedad Intelectual con enfoque práctico significa acercar el Derecho al trabajo real del abogado. No se trata de repetir artículos, sino de comprender cómo aplicar la ley 22.362 a casos concretos de registro, oposición o nulidad de marcas. Esta formación permite que los egresados puedan asesorar a empresas, emprendedores y pymes de su región, generando desarrollo profesional y evitando que los trámites se deriven a estudios fuera de la región.

El conocimiento técnico sobre el registro y la defensa de una marca representa una fuente de trabajo legítima y especializada. El abogado comercialista del NOA no solo interpreta la ley, sino que acompaña a los productores, artistas y diseñadores locales en el proceso de consolidar su identidad comercial. Esta perspectiva genera un círculo virtuoso: más capacitación jurídica, más confianza en los estudios regionales y una economía local más regulada.

Como destaca Lucarelli (2004), el docente universitario construye su identidad en un contexto de transformación permanente de su rol. En este proceso, la enseñanza del Derecho debe combinar rigor teórico con sensibilidad social y capacidad de innovación. Las universidades tienen un papel central en la producción de conocimiento social y regional, por lo que los docentes deben formarse también en el ámbito pedagógico, entendiendo que su tarea excede la transmisión de contenidos: forma profesionales y transforma territorios.

En la práctica, esta concepción implica repensar la enseñanza del Derecho Comercial como un campo interdisciplinario que articula economía, comunicación y tecnología. La Propiedad Intelectual, especialmente el derecho de marcas, es una herramienta jurídica que ordena el mercado y protege el esfuerzo creativo. Por eso, la docencia universitaria en este campo requiere una metodología que favorezca el aprendizaje significativo y el desarrollo de competencias: interpretar normas, analizar expedientes, usar plataformas digitales, argumentar con fundamento y aplicar principios éticos en la práctica.

En palabras de Maggio (2012), una enseñanza poderosa no solo transmite saberes, sino que genera debate y transforma a quienes aprenden. Desde esta visión, el aula jurídica se convierte en un espacio de experimentación, donde los alumnos enfrentan casos, discuten, se equivocan y corrigen, aprendiendo a pensar y actuar como profesionales. Esa es, precisamente, la esencia del método del caso aplicado al derecho de marcas.

3. La transformación digital del registro de marcas y los fundamentos pedagógicos

La transición del registro presencial al digital marcó un cambio estructural en la práctica profesional. Hasta hace pocos años, los abogados del interior debían trasladarse o recurrir a intermediarios en Buenos Aires para tramitar una marca. Hoy, el sistema del INPI permite realizar búsquedas, oposiciones y renovaciones completamente en línea, democratizando el acceso y reduciendo costos. Como señalan Delgado y Oliver (2012), la incorporación de las tecnologías de la información y la comunicación (TIC) en la enseñanza del Derecho supone mucho más que el uso instrumental de recursos digitales: implica una reconfiguración del acto educativo y de la cultura jurídica universitaria. La enseñanza del Derecho, tradicionalmente centrada en la oralidad y la transmisión normativa, se transforma en un proceso interactivo, colaborativo y tecnológicamente mediado, donde el conocimiento se construye de manera situada.

En este sentido, por ejemplo, el recurso de compartir pantalla durante una clase presencial, en línea o híbrida, constituye una práctica didáctica innovadora: permite al docente mostrar en tiempo real cómo acceder al portal del INPI, completar un formulario digital o analizar un expediente electrónico. Esta dinámica convierte la observación pasiva en una experiencia de aprendizaje activo y significativo, en la que el estudiante aprende haciendo. Para Delgado y Oliver, el desafío radica en formar juristas capaces de “leer el Derecho en clave tecnológica”, articulando el saber normativo con las habilidades digitales que hoy exige el ejercicio profesional.

En el aula, esta realidad exige un nuevo tipo de enseñanza: enseñar Derecho con tecnología. Los estudiantes deben aprender no solo a interpretar la ley, sino también a operar el entorno digital donde esa ley se aplica. Se utilizan capturas del sitio oficial del INPI, se simulan registros y se analizan ejemplos de marcas aceptadas o rechazadas. La virtualidad

se vuelve aliada del aprendizaje: los alumnos aprenden haciendo. Esta modalidad responde a los principios de la Didáctica General y Específica (Camilloni, 2007), que buscan articular el conocimiento teórico con las prácticas concretas de cada disciplina. En el caso del Derecho de Marcas, esto significa traducir la norma en acción, permitiendo que los futuros abogados comprendan el proceso administrativo y lo integren a su saber jurídico.

La incorporación de recursos digitales se complementa con herramientas de mapas mentales y conceptuales, que facilitan la organización del contenido y promueven la reflexión (Davini, 2015; Ritchhart *et al.*, 2014). Estos recursos ayudan a visualizar las relaciones entre conceptos como marca, titularidad, nulidad y oposición, favoreciendo el pensamiento crítico y el aprendizaje activo. Como destaca Anijovich (2014), la retroalimentación formativa es un eje fundamental de la evaluación universitaria: los docentes no solo califican, sino que acompañan el proceso de aprendizaje, brindando observaciones que permiten al alumno mejorar, reinterpretar y consolidar sus saberes. La evaluación deja de ser un fin y se convierte en una oportunidad de crecimiento.

Esta perspectiva coincide con el enfoque de evaluación deliberativa propuesto por Camilloni, Celman, Litwin y Palou de Mate (1998), que prioriza la comprensión de los procesos por sobre los resultados finales. La enseñanza se concibe como un espacio de diálogo y reflexión, donde el error es parte del aprendizaje. De este modo, la enseñanza de la Propiedad Intelectual en formato digital no solo moderniza contenidos, sino que transforma la relación pedagógica: el alumno se vuelve protagonista, el docente un facilitador, y el Derecho una herramienta viva de conocimiento y transformación social. Más aún cuando cada alumno que asiste a clases lleva un celular en la mano para seguir el ingreso a la página y buscar si una marca está o no registrada, pudiendo hacerlo mediante una transmisión proyectada en vivo, mientras el aula participa simultáneamente desde sus dispositivos o en modalidad en línea sincrónica.

4. El método del caso y la simulación pedagógica: “Cervecería La Fulanita”

El método del caso es una de las estrategias más eficaces para enseñar Derecho, porque permite aprender haciendo y pensando como jurista. En las clases de Derecho de las Empresas y los Negocios en la Universidad Nacional de Tucumán, se implementa un caso diseñado por la autora: “Cervecería La Fulanita”. Este caso simula un conflicto realista sobre la titularidad y el registro de una marca. Su trama –dos socios que crean una cerveza artesanal y descubren que la marca fue registrada a nombre de uno de ellos– permite aplicar directamente la Ley 22.362 sobre marcas, el procedimiento de registro ante el INPI y los principios de nulidad. A continuación, se presenta el resumen del caso docente:

Caso “Cervecería La Fulanita” (resumen pedagógico)

Javier y Antonella, estudiantes universitarios, fundan en 2012 un emprendimiento cervecero llamado La Fulanita, que crece hasta obtener premios y notoriedad. En 2019, Javier intenta registrar la marca, pero descubre que ya fue registrada a nombre de Antonella y Antonio, nuevo socio capitalista. Frente a esta situación, el alumno debe analizar qué ley

se aplica, qué procedimiento seguir y cómo asesorar jurídicamente a Javier para proteger su derecho.

Preguntas orientadoras:

1. ¿Qué ley se aplica al problema?
2. ¿Cómo se registró la marca y ante qué organismo?
3. ¿Cuándo y cómo debería haberse opuesto Javier?
4. ¿Quién resuelve la oposición y qué recursos existen?
5. ¿Qué asesoramiento brindarías como abogado/a de Javier?

Estas preguntas promueven el razonamiento jurídico, la argumentación y la búsqueda de soluciones viables. En el aula, los alumnos trabajan en grupos, exponen su posición y reciben retroalimentación guiada por la docente, aplicando los principios de la evaluación formativa (Steiman, 2008; Anijovich, 2014). El caso se complementa con actividades digitales: simulaciones de registro, videos cortos explicativos y búsquedas reales en el portal del INPI. Así, se combinan el aprendizaje técnico y el pensamiento reflexivo. Como explica Maggio (2012), una enseñanza transformadora no busca respuestas cerradas, sino abrir el debate y construir pensamiento jurídico autónomo. La Fulanita no pretende ofrecer una solución única, sino formar futuros abogados capaces de decidir con criterio y humanidad.

Como sostienen García y Fernández (2010), el método del caso constituye una de las estrategias más eficaces para la enseñanza del Derecho, porque promueve el desarrollo del razonamiento jurídico, la argumentación y la toma de decisiones éticamente fundadas. Su aplicación permite al estudiante asumir el rol del profesional, enfrentarse a problemas verosímiles y explorar la pluralidad de soluciones posibles. En este marco, el caso “Cervecería La Fulanita” se inscribe dentro de esta tradición pedagógica, en tanto traslada al aula los desafíos reales del ejercicio profesional, integrando análisis normativo, criterio técnico y reflexión ética. Del mismo modo, Maggio (2012) enfatiza que enseñar en la universidad implica abandonar la lógica de la transmisión para adoptar una lógica de mediación y construcción colectiva del conocimiento, donde el aula se concibe como un laboratorio de pensamiento crítico. La combinación del método del caso con recursos digitales –simulaciones, búsquedas en línea, proyección de formularios reales– potencia esta dimensión transformadora, generando aprendizajes profundos y socialmente relevantes.

5. Conceptos fundamentales para la práctica profesional

Comprender qué es una marca, cómo se registra y cuáles son sus límites resulta clave para ejercer con responsabilidad. Según la Ley 22.362, la marca es todo signo con capacidad distintiva para identificar productos o servicios. La enseñanza de este concepto debe centrarse en la función diferenciadora de la marca, su vínculo con la reputación comercial y su rol económico como bien inmaterial (Alterini, 1999).

En el aula, se enseña que no todo signo puede registrarse como marca: la ley prohíbe expresiones genéricas, engañosas o contrarias a la moral. A través del caso La Fulanita, los alumnos descubren que la elección de un nombre comercial implica responsabilidad y estrategia jurídica. Se analizan también las causas de nulidad: registros de mala fe, contravención a la ley o conocimiento previo de un tercero (art. 24, Ley 22.362).

El análisis práctico permite que los estudiantes comprendan el proceso de oposición y defensa ante el INPI, el papel de la Dirección Nacional de Marcas y el derecho de recurrir ante la Cámara Nacional de Apelaciones en lo Civil y Comercial Federal.

Estos ejercicios no solo enseñan procedimiento: forman criterio profesional. Los alumnos aprenden a advertir a sus futuros clientes sobre plazos, oposiciones y conflictos, fortaleciendo su capacidad de asesoramiento.

El Derecho de Marcas, enseñado así, deja de ser un tema abstracto para convertirse en una herramienta de trabajo y desarrollo regional. Los abogados formados en este enfoque no repiten definiciones: piensan jurídicamente, aplican la ley y comprenden su sentido económico y social.

6. Diferencias entre marca, patente, modelo y diseño industrial

Es fundamental para el ejercicio profesional y la enseñanza del Derecho Comercial comprender las diferencias entre los distintos derechos de Propiedad Industrial. Estas categorías –marca, patente, modelo y diseño industrial– se complementan entre sí, pero tienen objetivos y alcances distintos.

La marca, regulada por la Ley 22.362, protege el signo que distingue productos o servicios. Su función principal es identificar el origen y generar confianza en el consumidor. Por ejemplo, L’Oreal, Mercedes-Benz o McDonald’s son marcas registradas que representan prestigio y reconocimiento. Enseñar qué es una marca implica mostrar su valor simbólico y económico: la marca comunica identidad.

En cambio, una patente de invención, prevista en la Ley 24.481 (t.o. Decreto 260/96), protege un procedimiento técnico o una solución nueva con aplicación industrial. Es el caso del método de producción en serie desarrollado por Ford, o de ciertos procesos de elaboración rápida patentados por cadenas internacionales de comida. La patente no protege el nombre ni el diseño externo, sino la invención o procedimiento que produce un resultado novedoso.

Los modelos de utilidad protegen mejoras funcionales introducidas en objetos ya existentes. Son pequeños inventos o adaptaciones que los vuelven más útiles o cómodos. Por ejemplo, un sacacorchos con palanca, una planchita con control térmico o un termo que calienta el agua automáticamente son modelos de utilidad: aportan una mejora práctica a un objeto conocido: no se crea uno nuevo, se mejora uno existente que lo hace más útil.

Por su parte, los diseños industriales amparan la forma exterior y estética de un producto, su aspecto ornamental o visual. No protegen la funcionalidad, sino la apariencia que genera atracción o identidad. Pueden verse en ámbitos tan diversos como la moda o la industria automotriz: el diseño de una colección de alta costura o los automóviles de lujo, donde la estética y la forma exterior del vehículo son parte esencial del valor de marca y de la comunicación visual.

Enseñar estos ejemplos en el aula ayuda a que los estudiantes comprendan que el Derecho de la Propiedad Industrial también protege la creatividad visual y el diseño, no solo los in-

ventos o procedimientos. Como sostiene Etcheverry (2005), la Propiedad Industrial cumple una función social, al incentivar la innovación y garantizar transparencia en el mercado.

Desde la experiencia docente en el NOA, enseñar estas diferencias no solo es una cuestión técnica, sino una herramienta para el desarrollo profesional y territorial. Permite que los abogados locales puedan asesorar a empresas, artesanos, diseñadores o pymes que buscan proteger su trabajo sin depender de estudios de la capital. Así, la enseñanza jurídica se convierte también en una forma de arraigo y fortalecimiento de la economía regional.

7. Conclusión: enseñar propiedad intelectual para transformar la práctica profesional

Enseñar Derecho requiere vincular la norma con la vida. En el caso de la Propiedad Intelectual, esta tarea cobra un sentido especial: enseñar sobre marcas, patentes o modelos industriales es enseñar a proteger el fruto del ingenio, del trabajo y de la identidad.

En las provincias del NOA, donde la producción local y el emprendimiento crecen día a día, formar abogados que comprendan la aplicación práctica del Derecho de Marcas significa preparar profesionales capaces de acompañar ese desarrollo. La docencia universitaria en esta materia no debe limitarse a la teoría; debe ofrecer herramientas reales para que el Derecho se ponga al servicio de la comunidad.

El método del caso, utilizado en experiencias como “Cervecería La Fulanita”, es una propuesta que busca acercar el conocimiento a la realidad profesional. No pretende establecer un modelo único ni una verdad absoluta, sino invitar a reflexionar, debatir y aplicar la ley a situaciones posibles. En esa interacción, el alumno se convierte en protagonista del aprendizaje y el docente en guía que orienta con sentido crítico.

Formar abogados que piensen, argumenten y decidan con responsabilidad es una tarea que trasciende el aula. El Derecho, como ciencia social, necesita profesionales conscientes de su función ética y de su compromiso con el entorno. Enseñar Propiedad Intelectual, entonces, es enseñar a defender la creatividad, respetar el esfuerzo ajeno y valorar la originalidad humana. Cada marca, patente o diseño protegido representa no solo un bien jurídico, sino una historia detrás: el trabajo de alguien que creó, innovó o soñó. Desde el NOA, enseñar con esta mirada implica unir conocimiento, identidad y futuro.

Por eso, la enseñanza del Derecho de Marcas no es solo un tema más del plan de estudios. Es una manera de fortalecer la práctica profesional, dignificar el trabajo intelectual y afirmar que el Derecho –cuando se enseña con claridad y compromiso– puede ser también una herramienta de trabajo, desarrollo humano y regional.

Referencias

- Ahumada, P. (2005). *Evaluación de los aprendizajes en la educación superior*. Santiago de Chile: Editorial Universitaria.
- Alterini, A. (1999). *Derecho de las Obligaciones*. Buenos Aires: Abeledo Perrot.

- Anijovich, R. (2014). *La evaluación como oportunidad: hacia una mirada formativa en la enseñanza universitaria*. Buenos Aires: Paidós.
- Bertoni, M. (2000). *Evaluación y comunicación pedagógica*. Buenos Aires: Troquel.
- Camilloni, A. (2007). *La didáctica general y la didáctica específica*. Buenos Aires: Paidós.
- Camilloni, A., Celman, S., Litwin, E., & Palou de Mate, M. (1998). *La evaluación de los aprendizajes en el debate didáctico contemporáneo*. Buenos Aires: Paidós.
- Davini, M. C. (2015). *Métodos de enseñanza: didáctica general para maestros y profesores*. Buenos Aires: Santillana.
- Delgado, J., & Oliver, J. (2012). *Enseñanza del Derecho y tecnologías de la información y la comunicación*. Universitat Oberta de Catalunya (UOC).
- Etcheverry, R. (2005). *Derecho de la Propiedad Industrial*. Buenos Aires: Astrea.
- García, J., & Fernández, E. (2010). “El método del caso en la enseñanza del Derecho: fundamentos, diseño y aplicación didáctica”, *Revista de Educación y Derecho*, (2). Universidad de Barcelona.
- Lucarelli, E. (2004). *Prácticas innovadoras en la formación del docente universitario*. Buenos Aires: Paidós.
- Maggio, M. (2012). *Enseñar en la universidad: un oficio que se transforma*. Buenos Aires: Paidós.
- Ritchhart, R., Church, M., & Morrison, K. (2014). *Hacer visible el pensamiento*. Buenos Aires: Paidós.
- Steiman, J. (2008). *Evaluar para aprender: la evaluación formativa en la educación universitaria*. Córdoba: Brujas.

AUTOMATIZACIÓN DEL PROCESO JUDICIAL DE ALIMENTOS EN JUJUY

Toward an Automated Child Support Process in Jujuy's Judiciary

Franco Marcelo Bravo*

Universidad Nacional de Tucumán

drfrancobravo@gmail.com

RECIBIDO 22/10/2025 - ACEPTADO 17/11/2025

Resumen

Este artículo propone lineamientos de innovación para el proceso de alimentos en el fuero de Familia de la Provincia de Jujuy. En particular, plantea la automatización de la resolución de embargo provisorio mediante la concentración, en un solo acto procesal, de las principales peticiones iniciales: admisión de la demanda, control formal, apertura del proceso, apersonamiento profesional, embargo provisorio y oficios de ley. Con base en el principio de economía procesal, esta reconfiguración busca acelerar la emisión de la orden de embargo en favor de niños, niñas y adolescentes, fortaleciendo su acceso efectivo a la justicia y la tutela judicial de sujetos en situación de vulnerabilidad.

Palabras clave:

alimentos, automatización, procesos judiciales, sujetos vulnerables, gobernanza de datos, inteligencia artificial, tutela judicial efectiva.

Abstract

This article proposes innovation guidelines for child support proceedings in the Family Court of the Province of Jujuy. Specifically, it advances the automation of provisional garnishment orders by consolidating, into a single procedural act, the main initial filings: admission of the claim, formal review, initiation of proceedings, counsel's appearance, provisional garnishment, and statutory notices. Grounded in the principle of procedural economy, this streamlined structure seeks to expedite the issuance of provisional garnishment orders in favor of children and adolescents, thereby strengthening their effective access to justice and the judicial protection of individuals in situations of vulnerability.

Keywords:

child support, automation, judicial proceedings, vulnerable subjects, data governance, artificial intelligence, effective judicial protection.

1. Introducción: tutela judicial efectiva de sujetos vulnerables

Recientemente se realizaron sondeos sociales en torno a la percepción ciudadana sobre el funcionamiento actual del sistema de justicia, arrojando resultados de valoración predominantemente negativos. No obstante, esta apreciación no constituye un fenómeno reciente, sino una constante histórica en la relación entre la sociedad y el Poder Judicial, lo que ha generado una mayor desconfianza en el sistema.¹

* Abogado. Maestrando en Derecho Privado (UNSa). Posgrado en Inteligencia Artificial y Derecho (UBA). Diplomado en Innovación y Gestión Judicial Tecnológica (U. Champagnat). Posgrado en Derecho de las Familias, Infancia y Adolescencias (UNT). Coordinador de Gestión de Justicia en Ministerio de Gobierno y Justicia de Jujuy. Presidente del Instituto de Derecho Informático y TIC del Colegio de Abogados y Procuradores de Jujuy.

¹ Consúltase, por ejemplo, el sondeo analizado por Hernán Capiello para *La Nación* (15/02/2021).

Una de las críticas más persistentes de la ciudadanía refiere a la demora en la tramitación de los procesos judiciales, rasgo que ha configurado percepciones socialmente arraigadas y, en cierto modo, aceptadas por la población, como reproduce el conocido adagio según el cual “una justicia lenta no es justicia”, expresión que resume la tensión existente entre la formalidad del proceso y la efectividad real del derecho a una tutela judicial oportuna.

Si bien la percepción de todo aquel que ha transitado alguna vez un proceso judicial es subjetiva, la afirmación de que “una justicia lenta no es justicia” se va alejando de ser considerada una opinión, pues más bien, tiene fundamento en lo que llamamos “tutela judicial efectiva”. Dicha tutela está prevista en nuestra Constitución Nacional (Preámbulo y Art. 18 de la CN) como así también en los Tratados Internacionales con jerarquía constitucional (*cf.* Art. 75 inc. 22 de la CN) tales como la Declaración Universal de Derechos Humanos (arts. 10 y 11); la Declaración Americana sobre Derechos y Deberes del Hombre (art. 28); la Convención Americana sobre Derechos Humanos (arts. 8 y 9); Pacto Internacional de Derechos Económicos, Sociales y Culturales (art. 14); y la Convención sobre los Derechos del Niño (art. 40) entre otros. En particular, el art. 8. 1. de la Convención Interamericana de Derechos Humanos, dispone que: “Toda persona tiene derecho a ser oída, con las debidas garantías y dentro de un plazo razonable, por un juez o tribunal competente, independiente e imparcial, establecido con anterioridad por la ley, en la sustanciación de cualquier acusación penal formulada contra ella, o para la determinación de sus derechos y obligaciones de orden civil, laboral, fiscal o de cualquier otro carácter”. A su turno, la Declaración Americana de los Derechos y Deberes del Hombre señala en el art. 18 que: “Toda persona puede ocurrir a los tribunales para hacer valer sus derechos. Asimismo, debe disponer de un procedimiento sencillo y breve por el cual la justicia lo ampare contra actos de la autoridad que violen, en perjuicio suyo, alguno de los derechos fundamentales consagrados constitucionalmente”.

Ahora bien, dentro del diseño de procesos judiciales, existe un grupo de personas que merecen especial atención y un esfuerzo mayor por parte de los Estados para respetar los plazos razonables que imponen las normas constitucionales: ellos son los niños, niñas y adolescentes (NNA), personas con discapacidad y adultos mayores, que son sujetos agrupados por una homogeneidad de situaciones de vulnerabilidad: jurídica, social, económica, etaria, etcétera. En muchas ocasiones tales grupos son alcanzados por lo que en la jerga de los Derechos Humanos se llama “interseccionalidad” (Gebruers, 2020).

Las Cien Reglas de Brasilia sobre Acceso a la Justicia de las Personas en Condición de Vulnerabilidad, a las cuales la Corte Suprema de Justicia de la Nación ha adherido mediante Acordada 5/2009 –en el punto 25 correspondiente al Cap. II, titulado “Efectivo acceso a la justicia para la defensa de los derechos”–, disponen: “Se promoverán las condiciones necesarias para que la tutela judicial de los derechos reconocidos por el ordenamiento sea efectiva, adoptando aquellas medidas que mejor se adapten a cada condición de vulnerabilidad”.

En el mismo sentido, el Código Civil y Comercial de la Nación, legisla algunos principios generales de los procesos de familia, donde en el Art. 706 dispone: “El proceso en materia de familia debe respetar los principios de tutela judicial efectiva, intermediación, buena fe y

lealtad procesal, oficiosidad, oralidad y acceso limitado al expediente. Las normas que rigen el procedimiento deben ser aplicadas de modo de facilitar el acceso a la justicia, especialmente tratándose de personas vulnerables, y la resolución pacífica de los conflictos. Los jueces ante los cuales tramitan estas causas deben ser especializados y contar con apoyo multidisciplinario. La decisión que se dicte en un proceso en que están involucrados niños, niñas o adolescentes, deben tener en cuenta el interés superior de esas personas”.

Como vemos, la legislación actual nos interpela a garantizar con mayor énfasis el acceso a la justicia a los sectores más vulnerables de nuestra sociedad. Sin embargo, también es cierto que en muchas ocasiones nos encontramos con algunas barreras de tipo cultural, normativo, u organizacional, que impiden que los estrados judiciales puedan lograr una respuesta efectiva, con la celeridad con la que un NNA necesita cubrir sus necesidades básicas. Frente a ello, a continuación, se reseñan experiencias de uso ético y con supervisión humana, de incorporación de avances tecnológicos en la justicia, las que podrían servir para encontrar modelos o antecedentes de algunas soluciones a los actuales problemas de temporalidad en la misma.

2. Automatizar tareas con inteligencia artificial

Como vimos anteriormente, el estado actual de la mirada social sobre el funcionamiento de la justicia no es la mejor, siendo la “lentitud” un aspecto muy reclamado por las personas que pasaron por un proceso judicial. Frente a ello, se añade el desafío de mejorar los diseños de organización judicial para que el servicio de justicia sea más eficiente y eficaz.

Una de las herramientas para abordar estos desafíos, claramente es la incorporación a los procesos judiciales de las nuevas tecnologías de la información y comunicación (TIC). Estas últimas, usadas de manera responsable, supervisadas por defecto por los humanos, con principios de legalidad, explicabilidad, transparencia y evitando sesgos de distintos tipos en su creación, pueden traer grandes beneficios para mejorar la eficiencia y eficacia de la prestación del servicio de justicia.

Cuando hablamos de desarrollo tecnológico (IA, automatización, *blockchain*, *machine learning*, entre otros) aplicado a los procesos judiciales, entendemos que el mismo va a facilitar el acceso a la justicia de diferentes maneras: licuando en los algoritmos tareas rutinarias, repetitivas y mecánicas; posibilitando que la fuerza laboral pueda ser más productiva en tareas postergadas o más complejas, y/o reduciendo los tiempos de respuesta a los ciudadanos, entre otras.

En lo que respecta a este trabajo, quiero hacer foco en el camino hacia la automatización de tareas rutinarias con la utilización de dos herramientas útiles del diseño actual de los procesos judiciales: la gobernanza de datos y la automatización de tareas, las que utilizadas con herramientas de las nuevas TIC pueden comenzar a romper las barreras que impiden lograr una justicia más ágil para las personas.

Ahora bien, automatizar los procesos judiciales no significa reemplazar directamente a los valiosos integrantes u operadores judiciales, sino muy por el contrario, trae consigo la idea

de incorporar las herramientas de la tecnología, supervisadas por los humanos, para maximizar la producción del trabajo y minimizar los tiempos judiciales.²

En la actualidad, la automatización de tareas se muestra como un complemento que potencia y fortalece el trabajo humano. Aquí surge el concepto de “cobotización”, como una convergencia entre sistemas de IA, robots y trabajadores humanos o los llamados nuevos trabajadores digitales. Quizás, la idea central en este tipo de relaciones, sea crear una fuerza laboral con inteligencia aumentada. Sobre esta base, la inteligencia aumentada se basa en una cobotización inclusiva, que presupone dirigir los esfuerzos para establecer cuatro grandes herramientas que se aplican a los grandes sectores de las actividades humanas (industrial, manufactura y servicios, entre otras). Estas son: 1) asistencia inteligente; 2) automatización; 3) diagnóstico o detección inteligente; 4) predicción (Corvalán, 2019).

En este sentido, dos de los casos de comprobado éxito en la implementación de IA en la Justicia son, sin dudas, la experiencia Prometea³ y el caso de Pretoria⁴, dos sistemas enfocados a la actividad judicial que fueron desarrollados por el Laboratorio de Inteligencia Artificial y Derecho de la Universidad de Buenos Aires. En ambos casos, la aplicación de IA obtuvo como resultados, entre otros, la automatización de tareas repetitivas y la formulación de predicciones inteligentes, con los beneficios comprobados de una notable disminución de tiempos, trayendo consigo las ventajas que los empleados y funcionarios judiciales puedan dedicar más tiempos a casos más complejos, aquellos que requieran de un análisis más profundo y mayor presencia humana. Estas experiencias combinaron el trabajo colaborativo e interdisciplinario (abogados, programadores, diseñadoras, funcionarios y jueces) con un profundo estudio de la materia, que se sumaron a un eje estructural de todo el diseño: la decisión de mejorar nuestra justicia con proyectos factibles, que son adaptados a las realidades y necesidades judiciales de cada jurisdicción requirente.

Es por ello que, sentadas las nociones de automatización junto con la importancia de la tutela judicial efectiva en el proceso judicial de sujetos vulnerables, veamos cómo dicha automatización podría ser implementada en el Poder Judicial de Jujuy.

3. El proceso judicial de alimentos en el Poder Judicial de Jujuy

El proceso judicial de alimentos en la Provincia de Jujuy se encuentra regulado en la Ley Provincial N° 6.362 (Procesal de Familia), donde se establecen las reglas procedimentales del mismo, adoptando además principios procesales tales como la celeridad y economía procesal.

En el presente, nos enfocaremos en los llamados “Alimentos provisorios”, es decir, en la orden judicial que el Juez realiza para decretar la viabilidad de un embargo sobre los habe-

² Para profundizar en esta cuestión, ver Cevasco y Corvalán (2018).

³ Prometea es un sistema argentino de inteligencia artificial multicapa, desarrollado en conjunto por el Ministerio Público Fiscal de la Ciudad Autónoma de Buenos Aires y la Facultad de Derecho de la UBA, con el objetivo de agilizar la justicia y permitir un mejor uso de los recursos.

⁴ Para conocer más sobre Pretoria, consúltase Estévez *et al.* (2020).

res de un demandado –en relación de dependencia– deudor alimentario, con ingresos ciertos.⁵

Según la base de datos disponible en el portal de Datos Abiertos de la Justicia Argentina del Ministerio de Justicia de la Nación⁶, luego del análisis de los datos y causas no penales (civiles, laboral, familia, tributarios, etc.), referidos al Poder Judicial de Jujuy, se pueden extraer de forma preliminar algunas conclusiones en relación a nuestro tema:

- Con un 45,2%, los Procesos de Familia son el segundo fuero con más actividad judicial de todos los fueros no penales en Jujuy.
- El 20% de todos los juicios no penales en Jujuy son de alimentos.
- El 60% de los juicios dentro del fuero de familia, son expedientes de alimentos.
- A estos datos, deben sumarse algunas circunstancias que muchas veces ocasionan dilaciones en el trámite de alimentos, con la consecuencia de no poder minimizar los tiempos en este tipo de acciones que involucran NNA, tales como:
 - Vocalía o Juzgado de turno sin designación de jueces y/o juezas;
 - Desproporcionalidad entre el volumen de trabajo y la asignación de RRHH;
 - Circunstancias excepcionales como pandemias mundiales;
 - Ciberataques a los servidores informáticos de justicia;
 - Diseño judicial y/o errores materiales en los datos del expediente.

En este sentido, la obtención de una resolución judicial provisoria para satisfacer las necesidades de NNA, a través del llamado “embargo de alimentos provisorios”, lleva en promedio entre 2 a 4 semanas desde la interposición de demanda, sin contar las diligencias procesales que son necesarias para efectivizar dicha medida.

Consecuente con lo anterior, y a grandes rasgos, podemos decir que el trámite judicial para efectivizar una medida de embargo provisorio de alimentos en Jujuy, se compone en la actualidad de 5 pasos o actos procesales, según las actuales normas procesales que rigen este tipo de juicios⁷, las que podemos esquematizar del siguiente modo:

Nº Actos Procesales	Acto Procesal	Responsable
1º	INGRESO DE DEMANDA	ABOG. LITIGANTE
2º	DECRETO APERTURA/FIJAC. AUDIENCIA/ ORDEN DE EMBARGO	JUEZ/JUEZA
3º	INGRESO DE OFICIOS DE LEY p/ CONTROL Y FIRMA	ABOG. LITIGANTE

⁵ La segmentación obedece a que cuando se trata de pedidos de alimentos a progenitores que no cuentan con un trabajo registrado, los tiempos pueden variar más, debido a la difícil situación de saber su real ingreso, o en su caso saber quién es su empleador, entre otras variantes. En tales casos el análisis y las decisiones son diferentes.

⁶ Disponible en: <https://datos.jus.gob.ar/>

⁷ En la actualidad, el proceso sigue las normas del Juicio Abreviado, según Art. 34 de la Ley N° 6.362, Ley Procesal de Familia de Jujuy.

4°	FIRMA DE OFICIOS DE LEY (Empleador y Banco)	JUEZ/JUEZA
5°	DILIGENCIAMIENTO DE OFICIOS DE LEY	JUEZ: Oficio Banco ABOG.: Oficio Empleador

Figura 1: Diseño actual de actos procesales en un embargo provisorio de alimentos en la Provincia de Jujuy.
Fuente: Elaboración propia.

Así vemos que, en el actual diseño judicial del proceso de alimentos en Jujuy, los actos procesales previos a la operatividad del embargo judicial de alimentos provisorios son cinco. Es decir, los pasos procesales necesarios para que al empleador de un demandado –en relación de dependencia– quien es deudor de alimentos, le ingrese una orden de descuento salarial para dar cumplimiento con el derecho humano de alimentar a su hijo, conlleva un número de instancias que, analizadas y para el caso de estudio, podrían explicarse del siguiente modo:

Respecto de las intervenciones del Poder Judicial, con el actual diseño, son necesariamente dos: 1°) Decretar sobre la admisibilidad de la demanda, y 2°) en un acto posterior, firmar electrónicamente los oficios de ley, (los que por su parte ya ordenó en su anterior intervención).

De este análisis podemos extraer una primera reflexión y decir que: al decretarse la admisibilidad de demanda y con ella la orden de embargo de alimentos provisorios, deviene en un acto procesal innecesario requerir nuevamente una firma de documentos judiciales (los oficios y cédulas de notificación) que podrían firmarse en el acto mismo de la admisibilidad de demanda.

Por otro lado, los abogados litigantes, deben realizar necesariamente tres intervenciones en este proceso para dar eficacia a la orden de embargo provisorio de alimentos. Dos de las intervenciones son ante el órgano judicial:

- 1) La presentación de una Demanda de Alimentos, –y posteriormente declarada la admisibilidad de la misma–,
- 2) Un escrito judicial que acompañe los Oficios de Ley, que son: a) Oficio al Banco Judicial, b) Oficio al Empleador y c) las Cédulas de notificación que fueran menester, para que recién, en otro acto procesal, sean firmados por el Secretario y/o el Juez/Jueza del expediente de alimentos.
- 3) Finalmente, y una vez firmadas las diligencias judiciales, la tercera intervención por parte del abogado litigante se realiza ante instituciones no judiciales, es decir que para efectivizar el embargo provisorio de alimentos decretado, el letrado deberá diligenciar los oficios y cédulas judiciales ante los bancos oficiales para aperturas y pagos de las cuentas judiciales, como así también diligenciar el oficio que ordene al empleador del alimentante realizar los descuentos de haberes, en concepto de alimentos provisorios.

Como se puede observar, los procesos de alimentos inciden de forma sustancial en el fuero de familia de Jujuy, pues se consolida como el proceso que ocupa el mayor volumen de trabajo, la mayor cantidad de tiempo destinado en una jornada laboral, y los mayores recursos humanos empleados en comparación a todos los restantes procesos judiciales de dicho fuero.

En el mismo sentido, vimos cómo funciona (a grandes rasgos) el proceso y los actos procesales que en la actualidad son necesarios para efectivizar las órdenes de embargo de alimentos provisorios para los alimentantes en relación de dependencia laboral. Ahora bien, ¿cómo podríamos optimizar y mejorar los tiempos en estos procesos? Intentaremos proponer a continuación algunas soluciones al respecto.

4. Automatización del proceso judicial de alimentos en Jujuy

Cuando hablamos de automatización en el proceso judicial, debemos tener presente que para lograrla es clave desarrollar –entre otras cosas– una adecuada gobernanza de datos judiciales.⁸ Gobernar el dato es hacerlo interoperable y no estático, toda vez que, después de un proceso de recolección, almacenado y curado, se puedan utilizar los mismos datos que se disponen para simplificar las tareas internas de labor diaria, evitar equívocos, realizar estadísticas o inferencias y, en definitiva, “tomar decisiones”.

En el actual juicio de alimentos en Jujuy vemos un desafío en cuanto a la gobernanza e interoperabilidad de datos, toda vez que se observa en el inicio del proceso, tiempos que podrían reducirse con distinta planificación del trámite procesal respecto de los pedidos por cuota alimentaria.

Esta modificación en el diseño judicial del proceso engloba cambios en el sistema informático de gestión judicial, tanto desde el ingreso de demanda hasta el diseño de las tareas y actos procesales en el juzgado y/o en la oficina judicial, no descartando eventuales modificaciones reglamentarias que podrían ser dispuestas por la Suprema Corte de Justicia en su rol de órgano reglamentario de las leyes judiciales.

Ello sin perjuicio de que el propio Código Procesal Civil y Comercial de la Provincia (CPCC), a través de los principios procesales de economía, concentración, y celeridad procesal (arts. 11, 14 y 16), establece normas que fijaremos como fundamento legal de las alternativas que proponemos a continuación, las que, a modo enunciativo, están destinadas a mejorar los tiempos judiciales del proceso de alimentos. Entre ellas podemos mencionar a las siguientes:

1) *Ingreso de causas judiciales mediante formularios prediseñados por el Poder Judicial*. Dado que en la actualidad es posible el ingreso de demandas, sus contestaciones, escritos y diligencias judiciales de manera remota o virtual, a través de la plataforma digital de gestión judicial creada y administrada por el Poder Judicial de la Provincia de Jujuy⁹, se propone que junto al escrito de ingreso de Demandas de Alimentos en los Tribunales de Familia, se adjunten formularios de ingreso de causas, que contengan datos esenciales del proceso de

⁸ Para ampliar sobre este punto, cf. Le Fevre Cervini (2022).

⁹ Conforme Ley Provincial N° 6175 y Acordada del Superior Tribunal de Justicia de Jujuy N° 86/2020. Consúltese: <http://www.justiciajujuy.gov.ar/index.php/plataforma-digital-de-gestion-judicial>

alimentos, como podrían ser: carátula y número de expediente; nombre y apellido de las partes; D.N.I. y/o CUIL, domicilio de las partes que intervienen en el proceso, CUIL del empleador del pre-sunto alimentante, y todo otro dato que sea relevante disponer para su correcta, responsable y útil interoperabilidad en el sistema de gestión judicial digital. Todo ello, sin perjuicio de escalar la gestión en el sistema de gestión judicial electrónico, adoptando convenios con entidades tales como Registro Civil de la Provincia, ANSES, RENAPER, ARCA, obras sociales, etcétera, para sistematizar y unificar datos. Esta propuesta, podría solucionar los problemas concretos de:

- *Carga repetitiva de datos*: Posibilidad de que el empleado y/o funcionario del Poder Judicial, no tenga que escribir en cada acto procesal: decreto de apertura, Sentencias interlocutorias, Actas de audiencias, Sentencias Finales, Oficios y Cédulas Judiciales, constancias judiciales, etc., Es decir datos que son esenciales del proceso judicial (N° de expediente, nombre del Juzgado, año de inicio, etc.) que se encuentra tramitando.
- *Errores de tipeo de datos*: Elimina posibles e involuntarios errores de tipeo en datos esenciales de las partes (nombres, DNI, CUIL, etc.).
- *Demoras evitables en el proceso*: Por ejemplo, si en un Decreto de Apertura del Juicio de Alimentos se escriben mal los datos del demandado (nombres, DNI, CUIL, etc.), y el litigante advierte esta cuestión, este último deberá interponer una herramienta procesal denominada “aclaratoria”, prevista en los Códigos Procesales, por la cual se buscará que el órgano judicial corrija errores materiales, aclare o supla omisiones involuntarias, lo que en definitiva acarrea una mayor dilación en el proceso, desgaste judicial y un perjuicio a la operatividad de los derechos de NNA.

2) *Deber de colaboración de los profesionales*. Otra de las alternativas que propongo se refiere a que, en el ingreso de las demandas de alimentos, junto al formulario de ingreso de causas, los litigantes puedan acompañar –a modo de colaboración con el Tribunal o Juzgado¹⁰– los oficios dirigidos tanto al empleador del presunto alimentante denunciado, como también al banco oficial encargado de abrir la cuenta judicial donde se depositarán las sumas embargadas por alimentos.

Es de sentido común asumir que es el propio abogado que inicia la demanda el más interesado en contribuir con la celeridad de los trámites. Además, la práctica tribunalicia demuestra que, ya en el escrito mismo de la demanda, los abogados denuncian los datos tanto del alimentante como de su empleador, habiendo realizado previamente la investigación y corroboración de dichos datos. Por ello, simplificar y unificar actos procesales en el juicio de alimentos, a través de los formularios, lograría reducir los tiempos en favor de los NNA.

3) *Oficios prediseñados por defecto*. Las diligencias judiciales al empleador y al banco oficial, deberían encontrarse por defecto en el sistema de expediente electrónico, prediseñadas con un formato estándar en modelos diseñados y aceptados en pleno por el Tribunal o Juzgado de Familia en cuestión. Ello con el fin de unificar criterios de aceptación y con

¹⁰ Artículo 63 del CPCC de Jujuy.

ello evitar dilatar el proceso con omisiones materiales, de formato en su confección o creación¹¹, o bien que no se ajuste al estilo forense de la Vocalía o Juzgado que lleve el trámite. De este modo, el profesional litigante sólo debería cargar los datos referidos a, por ejemplo, CUIT del empleador, nombre y DNI del demandado a pagar alimentos, lugar de domicilio, entre otros datos. Así, con esa organización y gestión judicial, se evitarían errores en el número de expediente o datos numéricos al respecto.

4) *Concentración de actos procesales*. Por su parte, tal y como lo vimos en párrafos precedentes, en el actual diseño del trámite judicial del proceso de alimentos, para llegar a obtener la operatividad de una orden de embargo provisorio, se deben realizar 5 pasos o actos procesales. Sin embargo, dicho trámite podría mejorar en cuanto a sus tiempos, si se concentrara en una misma resolución, la decisión respecto de los siguientes actos procesales:

- a) Admisibilidad de las cuestiones procesales de forma (personería, control de sellados y estampillados profesionales y/o previsionales, etc.); y también de las cuestiones de fondo (capacidad, parentesco, etc.).
- b) Admisibilidad del pedido de embargo de alimentos provisorios.
- c) Control y firma de las diligencias de ley (Oficios y Cédulas de Notificación), por parte del Juzgado o Tribunal de Familia.

Si bien escapa al análisis del presente trabajo, es importante destacar que en la actualidad existen programas de control de requisitos formales y sustanciales para la admisibilidad de actos jurídicos, lo que resulta una valiosa optimización de tiempos en la oficina para los operadores del sistema (Estévez *et al.*, 2020).

Nº Actos Procesales	Acto Procesal	Responsable
1º	INGRESO DE DEMANDA + OFICIOS DE LEY p/ CONTROL Y FIRMA (Cédula Notificación, Oficios Empleador y Banco)	ABOG. LITIGANTE
2º	DECRETO APERTURA/FIJAC. AUDIENCIA/ ORDEN DE EMBARGO + FIRMA DE OFICIOS	JUEZ/JUEZA
3º	DILIGENCIAMIENTO DE OFICIOS DE LEY	JUEZ: Oficio Banco ABOG.: Oficio Empleador

Figura 2: Propuesta de diseño y simplificación de actos procesales para lograr la efectividad de embargo provisorio de alimentos en la Provincia de Jujuy. Fuente: Elaboración propia.

El Tribunal o Juzgado a cargo podría realizar el control y firma respectiva de los oficios de ley, devenida de la interoperabilidad de los datos de los formularios de ingreso de causas, que se generaría de forma automática por parte del sistema digital del Poder Judicial. En este sentido, es importante señalar que, admitido el pedido de embargo de alimentos

¹¹ Al existir documentos estandarizados y aprobados por el Poder Judicial, se unificarían los criterios de aceptación y corrección de oficios, a su vez evitarían las interposiciones de recursos o aclaratorias procesales solicitadas por los litigantes.

provisorio, deviene automática la autorización del libramiento de oficios y cédulas de ley. Cabe resaltar que, si bien en la actualidad los actos procesales descriptos, son realizados y enviados a través de la plataforma digital del órgano judicial, el trámite se presenta disgregado en partes, y tal como vimos, bien podrían concentrarse/unificarse para optimizar tiempos y recursos.

Estructurar el proceso de alimentos con la posibilidad de ingresar en el mismo acto de interposición de demanda, los oficios de ley, eliminaría la innecesariedad de que los litigantes y operadores judiciales vuelvan a analizar un tema que podría haber sido resuelto desde su primera presentación. Tanto el oficio al banco para la apertura y pago de los fondos a depositarse, como los oficios al empleador del alimentante, pueden ser firmados por el Juez a cargo del expediente desde la primera presentación. El diseño judicial interno podría unificar actos, y entonces el trámite podría simplificarse, pasando de 5 a 3 actos procesales (como se ve en la Figura 2).

De esta manera, lograríamos reducir de 5 a 3 los actos procesales necesarios para obtener la eficacia y ejecutoriedad real de la resolución de embargo por alimentos provisorios, con todas las diligencias procesales firmadas y controladas por el órgano judicial en el acto mismo de la presentación de demanda.

Si bien el diseño que se propone, como se dijo anteriormente, está enfocado en el caso de un alimentante en relación de dependencia, que tiene ingresos formales y de un empleador al que se conoce el domicilio laboral, no por ello deja de ser una solución a un gran porcentaje de casos en la labor diaria del despacho judicial.

Finalmente, el diseño propuesto tiene la intención de optimizar los tiempos en el juicio de alimentos, atendiendo el reclamo de los justiciables y la tan ansiada celeridad de la justicia. Por otro lado, se volverían totalmente operativos los principios de economía, concentración y celeridad procesal del CPCC de Jujuy. Además, se aportarían alternativas para efficientizar el servicio de justicia, y con ello, acercarnos al cumplimiento de la tan anhelada tutela judicial efectiva y acceso a la justicia en favor de NNA y personas con discapacidad que requieran los servicios del Poder Judicial de Jujuy.

5. Conclusiones

La decisión de mejorar el servicio de justicia no es algo que sólo incumbe a los abogados, ni que depende exclusivamente de las cortes o tribunales de justicia; se trata de un esfuerzo compartido y de un trabajo colaborativo entre operadores jurídicos/ciudadanos/Estado. Las discusiones de política pública deben tener en el centro a las personas, sus contextos y sus problemas, ya que ello garantizará que surja un espectro de soluciones más amplio y efectivo. Utilizar la tecnología para mejorar la calidad de vida de las personas es una meta realizable y no utópica, ya que en varios países del mundo y en varias provincias de nuestro país, se están dando cambios significativos en materia judicial.

En el caso particular del fuero de familia, que tiene como sujetos de derechos a NNA, mayores de edad y personas con discapacidad, surge con mayor premura el replanteo de los diseños procesales para buscar mejoras de eficacia y eficiencia en favor de los sujetos

vulnerables a quienes se intenta proteger. Pero, también, es importante aplicar cuestiones como el análisis de datos judiciales, las experiencias y opiniones de los justiciables, un cambio de mentalidad o *mindset* en la prestación del servicio, y la ayuda de la tecnológica para eliminar las tareas repetitivas y destinar los valiosos aportes de los RRHH a tareas más complejas que demanda el fuero.

Innovar en cuestiones judiciales como las del presente, poniendo el foco de atención en uno de los colectivos de mayor vulnerabilidad como NNA es dar operatividad a la tutela judicial efectiva, que surge de los mandatos constitucionales e internacionales suscriptos por nuestro país. A su vez, estas innovaciones en el diseño procesal, son lo que llamamos “debido proceso algorítmico”, que para este autor significa brindar operatividad a principios procesales como economía, celeridad, concentración, a través del correcto uso de la tecnología en la justicia.

Finalmente, y como vimos, el desafío de volver más eficiente el servicio de justicia puede ser abordado, por supuesto, con los innegables beneficios de las nuevas tecnologías de la información y comunicación. Pero es importante recordar que antes de incorporar tecnología a la justicia, tengamos bien en claro por dónde empezar y a quiénes queremos proteger. Ello pues, detrás de cada caso o expediente judicial, están siempre las personas, y dicha sensibilidad aumenta cuando se trata de sujetos en condición de vulnerabilidad. Solo teniendo en claro que el centro de todo el diseño de justicia no es la ley, no son las formas sacramentales de los procesos, no somos los abogados o jueces, sino siempre y en todo momento las personas de cada expediente, recién entonces, podremos dedicarnos a buscar soluciones en la tecnología para mejorar nuestra justicia, nuestro trabajo, nuestra tutela judicial efectiva, en definitiva, nuestra vida.

Referencias

Amunátegui Perelló, C.; Madrid, R. (2020). “Sesgo e Inferencia en Redes Neuronales ante el Derecho”, en C. Aguerre, (Ed.). *Inteligencia Artificial en América Latina y el Caribe*. Ética, Gobernanza y Políticas. Buenos Aires: CETyS Universidad de San Andrés.

CAF. (2021). *Experiencia: Datos e Inteligencia Artificial en el sector público*. Caracas: CAF. Disponible en: <https://scioteca.caf.com/handle/123456789/1793>

Cappiello, H. (2021). “Tribunales en la mira: ocho de cada diez argentinos no confían en la Justicia”, *La Nación*, 15/02/2021, disponible en: <https://www.lanacion.com.ar/politica/ocho-cada-diez-argentinos-no-confia-justicia-nid2603178/>

CEJA. (2024). Revista N° 24, *Justicia y Tecnología*. Publicación anual del CEJA e INECIP.

CEJA. (2025). Revista N° 25, *Gestión Judicial desde la Práctica: una perspectiva integral sobre la administración de justicia*. Publicación anual de CEJA e INECIP.

Cevasco, L. y Corvalán, J. G. (2018). “¿Desempleo tecnológico? El impacto de la inteligencia artificial y la robótica en el trabajo”. LA LEY 11/07/2018, 1: AR/DOC/1329/2018.

Corvalán, J. G. (2021) *Tratado de inteligencia artificial y derecho*, tomo I / Juan G. Corvalán. (1a ed.), Ciudad Autónoma de Buenos Aires: La Ley, ISBN 978-987-03-4152-9.

Estévez, E.; Fillottrani, P.; Linares Lejarraga, S. (2020). “PROMETEA: Transformando la administración de justicia con herramientas de inteligencia artificial”, BID: <http://dx.doi.org/10.18235/0002378>

- Gebruers, C. (2020). “La noción de interseccionalidad: desde la teoría a la ley y la práctica en el ámbito de los derechos humanos”. *Perspectivas De Las Ciencias Económicas Y Jurídicas*, 11. Disponible en: <https://doi.org/10.19137/perspectivas-2021-v11n1a04>
- Lavin, R., Cristallo, J., Sánchez Caparrós, M. y Corvalán, J. G. (2024). “Uso de inteligencia artificial en los procesos judiciales: los juicios ejecutivos como oportunidad”. Fundar.
- Le Fevre Cervini, E. (2022). “Uso estratégico de datos e inteligencia artificial en la justicia”. Informe 6. Caracas: CAF. Disponible en: <https://scioteca.caf.com/handle/123456789/1932>
- Naciones Unidas, Departamento de Asuntos Económicos y Sociales (2012). “Estudio de las Naciones Unidas sobre el Gobierno Electrónico. Gobierno electrónico para el pueblo”. Disponible en: <https://publicadministration.desa.un.org/publications/e-government-people>
- Naciones Unidas, Consejo Económico y Social (2016). “Foro de múltiples interesados sobre la ciencia, la tecnología y la innovación en pro de los Objetivos de Desarrollo Sostenible”, Res. E/HLPF/2016/6, disponible en: https://digitallibrary.un.org/record/833657/files/E_HLPF_2016_6-ES.pdf
- Rodata, S. (2014). *El Derecho a tener derechos*. Editorial Trotta. Traducción de José Manuel Revuelta López.
- Sá Zeichen, G. (2018). Cuaderno de Derecho Judicial 28: Sistema de Justicia y Gobierno Abierto: “¿Es viable una Justicia Abierta?”. Buenos Aires: La Ley.
- Schwab, K. (2016). *La cuarta revolución industrial*. Ed. Debate, Barcelona.

EL ROL DE LA VÍCTIMA EN LA AUDIENCIA DE LIBERTAD CONDICIONAL: CONFLICTO ENTRE LA TUTELA EFECTIVA Y EL DEBIDO PROCESO EN JUJUY

The Victim's Role in Parole Hearings: Tension Between Effective Protection and Due Process in Jujuy

Mario de la Quintana*

Universidad Nacional de Jujuy

mariodelaq@gmail.com

RECIBIDO 18/10/2025 - ACEPTADO 17/11/2025

Resumen

El artículo analiza la participación de la víctima en las audiencias de libertad condicional, en el marco de la tensión entre su derecho a la tutela efectiva y las garantías del debido proceso del condenado. Se examinan las normas nacionales, provinciales y los estándares interamericanos aplicables, junto con la práctica judicial en Jujuy. Se sostiene que la intervención de la víctima debe orientarse a garantizar su seguridad y dignidad, sin desnaturalizar la finalidad resocializadora de la pena. Se proponen criterios prácticos para compatibilizar ambos derechos en las audiencias de ejecución.

Palabras clave:

víctima, libertad condicional, ejecución penal, tutela judicial efectiva, debido proceso.

Abstract

This article analyzes the participation of victims in parole hearings, within the tension between their right to effective protection and the convict's due process guarantees. It examines national and provincial regulations, as well as inter-American standards and judicial practice in Jujuy. It argues that victim participation should aim to ensure security and dignity without undermining the rehabilitative purpose of punishment. Practical criteria are proposed to balance both rights in sentence enforcement hearings.

Keywords:

victim, parole, criminal enforcement, effective protection, due process.

1. Introducción

El reconocimiento progresivo de los derechos de las víctimas ha transformado la estructura del proceso penal. Las reformas impulsadas a nivel nacional e internacional incorporaron nuevas formas de participación de quienes sufren el delito, desplazando la visión tradicional que las relegaba a un papel meramente pasivo. Este cambio, positivo en términos de acceso a la justicia, plantea desafíos específicos en la etapa de ejecución de la

* Abogado (Universidad Nacional de Tucumán), maestrando en Derecho Penal (Universidad Nacional de Rosario). Jefe de trabajos prácticos (UNJU). Actualmente se desempeña como Secretario de Ejecución de la Pena en el Poder Judicial de Jujuy.

pena, donde el centro de gravedad del proceso se traslada desde la verificación del hecho y la culpabilidad hacia el control del cumplimiento de la pena y su finalidad resocializadora.

En este contexto, la audiencia de libertad condicional representa un punto de fricción: allí confluyen, por un lado, el derecho de la víctima a ser oída y protegida, y por otro, las garantías constitucionales del condenado a un debido proceso y a la legalidad en la ejecución. La práctica judicial muestra que el equilibrio entre ambos derechos no siempre resulta claro, generando conflictos interpretativos que requieren pautas de actuación precisas.

El presente trabajo aborda este problema desde una perspectiva práctica y judicial, centrada en la experiencia de la Provincia de Jujuy. Se parte de la pregunta sobre si la tutela efectiva de la víctima incluye la facultad de ofrecer prueba para acreditar su vulnerabilidad y solicitar medidas de protección, o si su intervención debe limitarse a ser notificada y oída, sin capacidad probatoria activa. Para ello, se examinarán las normas nacionales y provinciales vigentes, los estándares internacionales de derechos humanos, y la jurisprudencia relevante. Luego, se propondrán criterios interpretativos orientados a fortalecer la seguridad de la víctima sin desnaturalizar la finalidad resocializadora de la pena ni vulnerar los derechos del condenado.

2. Tutela efectiva y debido proceso

La etapa de ejecución de la pena tiene un carácter eminentemente técnico, con un fuerte contenido garantista. Su finalidad es controlar que el cumplimiento de la sanción se realice conforme a los principios constitucionales y a la legalidad penal (Zaffaroni, 2011). Tradicionalmente, el eje de protección se concentró en el condenado, garantizando que la ejecución no se convierta en una prolongación arbitraria del poder punitivo.

Sin embargo, en las últimas décadas se incorporó un nuevo actor procesal: la víctima, quien reclama ser oída también en esta fase del proceso. Este reconocimiento, que se afianza tras la reforma constitucional de 1994 y la jerarquización de los tratados internacionales de derechos humanos (art. 75 inc. 22 CN), generó un nuevo escenario de tensión.

En particular, la reforma introducida por la Ley 27.375 a la Ley 24.660 de Ejecución de la Pena Privativa de la Libertad incorporó el artículo 11 bis, que otorga a la víctima el derecho a ser informada, expresar su opinión y proponer peritos en las audiencias donde se discutan beneficios de libertad. A primera vista, este derecho parece habilitar una intervención amplia. Sin embargo, en la práctica judicial surgen dos interrogantes. Primero, ¿puede la víctima ofrecer y producir prueba destinada a oponerse al otorgamiento de la libertad condicional, o su participación debe limitarse a manifestar su posición y acreditar su situación de vulnerabilidad? Segundo, ¿resulta aplicable este artículo en la Provincia de Jujuy, que no ha adherido a las reformas introducidas por la Ley 27.375?

Ambas cuestiones convergen en un mismo núcleo problemático: cómo compatibilizar la tutela efectiva de la víctima con las garantías del debido proceso del condenado, evitando que la audiencia de libertad condicional se transforme en una reedición del juicio de culpabilidad o en un nuevo espacio de revictimización.

3. Marco teórico y normativo

3.1. Fundamento constitucional e internacional

El artículo 18 de la Constitución Nacional asegura el derecho al debido proceso y la inviolabilidad de la defensa en juicio. Estos principios se proyectan sobre todas las etapas del proceso penal, incluida la ejecución de la pena. La Convención Americana sobre Derechos Humanos (CADH), en su artículo 8, refuerza este derecho, garantizando la legalidad y previsibilidad en la aplicación y modificación de las penas.

Paralelamente, el reconocimiento del derecho de las víctimas a participar activamente en el proceso deriva de instrumentos internacionales como la Convención de Belém do Pará (1994), que obliga a los Estados a proteger a las mujeres víctimas de violencia en todas las etapas judiciales; la Declaración de las Naciones Unidas sobre los Principios Fundamentales de Justicia para las Víctimas de Delitos y del Abuso de Poder (ONU, 1985), que reconoce el derecho a ser escuchadas y a obtener protección eficaz; y la jurisprudencia de la Corte Interamericana de Derechos Humanos, que en casos como *Bulacio vs. Argentina* (2003) y *González y otras ("Campo Algodonero") vs. México* (2009) afirmó que la víctima debe tener “pleno acceso y capacidad de actuar en todas las etapas” del proceso.

3.2. Normativa nacional

El marco legal argentino que regula los derechos de las víctimas en la ejecución penal se estructura sobre tres pilares:

- Ley 27.372 (Derechos y Garantías de las Víctimas de Delitos), cuyo artículo 6 otorga el derecho a ser notificadas y a manifestarse en audiencias de libertad condicional.
- Ley 24.660, modificada por la Ley 27.375, cuyo artículo 11 bis dispone expresamente que la víctima podrá ser informada, expresar su opinión y proponer peritos cuando se discuta la externación del condenado.
- Código Penal, que regula los requisitos materiales de la libertad condicional, destacando su carácter de derecho del condenado sujeto al cumplimiento de condiciones objetivas y subjetivas.

La interpretación sistemática de estas normas debe hacerse a la luz del principio de resocialización de la pena (artículo 5.6 de la CADH y artículo 10 del Pacto Internacional de Derechos Civiles y Políticos), que constituye la finalidad primordial de la ejecución penal.

3.3. Normativa provincial

El Código Procesal Penal de la Provincia de Jujuy (Ley 6.259 reformada por Ley 6.400) reconoce en su artículo 129 los derechos de la víctima, entre ellos: “ser escuchada antes de cada decisión que implique la extinción o suspensión de la acción penal” y “ser oída en las audiencias donde se decida sobre beneficios en la ejecución de pena que importen su soltura anticipada”.

Asimismo, el artículo 132 inciso d) establece que la situación de la víctima será tenida en cuenta “en oportunidad de modificar la medida o forma de cumplimiento de la pena”. Finalmente, el artículo 498 dispone que el juez de ejecución resolverá las solicitudes de libertad condicional “previo escuchar a las partes y a la víctima”.

No obstante, a diferencia del artículo 11 bis de la Ley 24.660, la normativa jujeña no prevé expresamente la facultad de ofrecer prueba. Esto abre un margen interpretativo para determinar si el derecho a ser “oída” puede incluir la posibilidad de acompañar elementos que acrediten su vulnerabilidad, sin que ello implique la producción probatoria en sentido estricto.

3.4. Perspectiva doctrinaria

La doctrina penal contemporánea coincide en que la etapa de ejecución de la pena no puede concebirse como una prolongación del castigo, sino como una fase autónoma orientada a la resocialización del condenado. Este principio, recogido en los tratados internacionales con jerarquía constitucional, constituye la base para delimitar el alcance de la intervención judicial y la participación de otros actores procesales, incluidas las víctimas.

Eugenio Zaffaroni sostiene que “la ejecución penal constituye el punto más delicado de la relación entre el Estado y la persona condenada, porque allí se define si el poder punitivo se mantiene dentro de la legalidad o se convierte en un ejercicio arbitrario” (Zaffaroni, 2011, p. 45). El autor subraya que el respeto al debido proceso en la ejecución no es una cuestión formal, sino una garantía sustancial frente a la expansión del poder punitivo estatal. Por ello, advierte que cualquier intento de “repolitizar” la ejecución a través de presiones sociales o simbólicas, como la intervención excesiva de la víctima o del clamor público, puede desnaturalizar el fin resocializador de la pena y convertir al juez en un mero ejecutor de demandas punitivas.

En el mismo sentido, Julio Maier recuerda que “la pena no es un acto de venganza ni un medio de reafirmación moral, sino una medida de control jurídico que debe orientarse hacia la reintegración del condenado a la comunidad” (Maier, 2004, p. 612). Según Maier, la ejecución es una etapa “puramente jurídica”, no sujeta a criterios de oportunidad política ni a valoraciones emocionales del delito o del daño. De allí deriva su afirmación de que “las audiencias de libertad condicional deben mantener su carácter técnico, evitando introducir en ellas debates morales o sentimentales” (*op. cit.*, p. 617).

Por su parte, Alberto Binder profundiza el análisis del rol judicial en esta fase. Destaca que el juez de ejecución no puede actuar como “administrador del castigo”, sino como “garante de legalidad frente al poder penitenciario” (Binder, 2013, p. 294). Esa función garantista implica asegurar tanto los derechos del condenado como los de la víctima, pero dentro de los límites del *ius puniendi*: “el juez no debe ser el gestor del castigo, ni el representante de la víctima, sino el árbitro de la legalidad; su tarea es controlar que la pena se cumpla en los términos previstos y cesar cuando su función resocializadora haya sido alcanzada” (*op. cit.*, p. 298).

Desde una visión complementaria, Edgardo Donna vincula la resocialización con el concepto de dignidad humana y la prevención especial positiva. En su criterio, el proceso de ejecución debe procurar que el condenado “recupere su capacidad de convivencia social” (Donna, 2019, p. 435). No obstante, advierte que esta finalidad no puede ser excusa para desatender la seguridad de la víctima, pues “la resocialización no es incompatible con la tutela, sino con la venganza” (*op. cit.*, p. 440).

En cuanto al equilibrio entre derechos, Alberto Bovino sostiene que la incorporación de la víctima al proceso penal es un avance democrático, pero debe estructurarse “de modo que no afecte la presunción de inocencia ni las garantías del debido proceso” (Bovino, 2015, p. 173). En materia de ejecución, sugiere un modelo de “participación informada”, donde la víctima puede expresar su situación y solicitar protección, sin intervenir en la valoración de la conducta penitenciaria. Para Bovino, “la intervención emocional en esta etapa erosiona la racionalidad jurídica y desdibuja el rol del juez como garante de la legalidad” (*op. cit.*, p. 176).

Desde una mirada latinoamericana, Carlos Tiffer plantea que la ejecución penal es un espacio donde se concretan los derechos humanos del condenado, de las víctimas y de la sociedad. Por ello, el juez debe ejercer un “rol de equilibrio” entre la seguridad ciudadana y la reinserción social, entendiendo que la verdadera finalidad del sistema no es prolongar el encierro, sino reducir los factores que generan reincidencia. “El juez de ejecución es un mediador de garantías: debe oír a la víctima, pero también recordar que el Estado no castiga para destruir, sino para reinsertar. Toda decisión que olvide esa finalidad pierde legitimidad constitucional” (Tiffer, 2020, p. 52).

Estas posiciones doctrinarias convergen en un punto común: la función judicial de control del poder punitivo. La víctima puede y debe ser oída, pero su participación no puede reabrir el debate sobre la culpabilidad, ni interferir con la evaluación técnica del cumplimiento de la pena. El juez de ejecución, como garante de los derechos de todos los intervinientes, debe situarse en un punto de equilibrio: ni indiferente al sufrimiento de la víctima, ni rehén de la demanda punitiva.

En definitiva, la doctrina penal contemporánea enseña que la resocialización del condenado y la protección efectiva de la víctima no son objetivos antagónicos, sino complementarios dentro de un modelo de justicia restaurativa y racional. El desafío institucional radica en asegurar que ambos derechos se ejerzan dentro de los límites del *ius puniendi* legítimo, evitando que la ejecución penal se convierta en una extensión simbólica del castigo o en un ámbito de revictimización.

4. Análisis del conflicto en la etapa de ejecución penal

4.1. La audiencia de libertad condicional como espacio de control técnico

La audiencia de libertad condicional no constituye una instancia de revisión de la culpabilidad ni de la pena impuesta. Su objeto es verificar si el condenado cumple con los requisitos legales, objetivos y subjetivos, para acceder al beneficio (art. 13 CP), y no se encuentre entre los delitos excluidos del art 14 CP. La función del juez de ejecución es eminentemente técnico-garantista, centrada en la observancia del principio de legalidad y la finalidad resocializadora de la pena (Maier, 2004).

En este marco, la participación de la víctima debe entenderse de manera acotada y funcional al propósito del instituto. Si se permitiera su intervención para introducir pruebas que revaloricen la peligrosidad o la gravedad del hecho, se correría el riesgo de reabrir el juicio de culpabilidad, vulnerando el principio de cosa juzgada. La Corte Suprema de Justicia de la Nación en el precedente *Bustos, Juan Carlos s/ recurso de casación* (2016) dejó en claro que

la libertad condicional es un derecho del condenado que nace del cumplimiento de requisitos objetivos, no de una facultad discrecional del juez, ni de la voluntad de la víctima. Cualquier limitación basada exclusivamente en la oposición de ésta resultaría incompatible con el principio de legalidad penal.

En la práctica judicial, sin embargo, la víctima puede y debe tener un rol activo para garantizar su seguridad personal. Ello no significa que participe en la valoración de la conducta penitenciaria o en la evaluación técnica de los informes criminológicos, sino que puede aportar elementos que permitan al tribunal disponer medidas de protección adecuadas frente a una eventual liberación.

4.2. Límites y alcances de la participación de la víctima

El juez de ejecución debe diferenciar entre dos planos normativos y funcionales distintos:

- 1) Plano del cumplimiento de los requisitos legales del beneficio (propio del condenado).
- 2) Plano de la protección personal de la víctima (propio del interés tutelar).

El primero se rige por las garantías del debido proceso y la legalidad penal. El segundo, por el derecho a la tutela efectiva reconocido en la Constitución, los tratados internacionales y las leyes nacionales. En consecuencia, la intervención de la víctima puede y debe orientarse a su protección, pero sin invadir la evaluación del cumplimiento de los requisitos legales de la libertad condicional.

La Ley 27.372 y el artículo 132 del CPP Jujuy habilitan al juez a tener en cuenta la situación de la víctima al modificar la forma de cumplimiento de la pena. Esto incluye ponderar circunstancias de vulnerabilidad comprobadas (por ejemplo, residir en el mismo barrio que el condenado, haber sufrido amenazas o padecer secuelas psicológicas graves).

Así, la víctima puede acompañar informes psicológicos, sociales o policiales que acrediten riesgos específicos, pero estos elementos deben valorarse exclusivamente a los fines de adoptar medidas de protección (como prohibición de acercamiento, cambio de residencia del liberado o dispositivos de control electrónico), sin afectar el derecho del condenado a la libertad condicional si cumple con los requisitos legales.

En términos prácticos, el juez de ejecución puede aplicar una doble resolución: en primer lugar, decidir sobre el otorgamiento del beneficio, con base en criterios objetivos y, en segundo lugar, fijar condiciones especiales de cumplimiento que aseguren la protección de la víctima, de acuerdo con los elementos aportados.

4.3. Aplicabilidad del artículo 11 bis de la Ley 24.660 en Jujuy

La cuestión sobre la aplicabilidad del artículo 11 bis incorporado a la Ley 24.660 por la Ley 27.375 en el ámbito provincial reviste particular trascendencia práctica, dado que dicho precepto introduce la participación directa de la víctima en las audiencias de ejecución, incluyendo la facultad de proponer peritos.

El punto de partida para el análisis debe ser el principio federal de autonomía procesal (arts. 121 y 126 de la Constitución Nacional), según el cual las provincias conservan todo el poder no delegado al Estado nacional, entre ellos la regulación procesal penal y la organi-

zación del Poder Judicial local. Ello implica que las normas de contenido formal o procedimental dictadas por el Congreso Nacional rigen únicamente para el fuero federal, salvo adhesión expresa de las provincias.

En consecuencia, la Ley 27.375, que reformó la Ley nacional de Ejecución de la Pena Privativa de la Libertad (Ley 24.660), salvo en las normas que modifican el Código Penal, no tiene aplicación automática en las jurisdicciones provinciales, salvo que estas incorporen sus disposiciones por vía de adhesión legislativa y así lo dice expresamente el art. 41 de la propia 27.375, que reforma el art. 228 de la Ley 24.660, el cual quedó redactado de la siguiente manera: “La Nación procederá a readecuar la legislación y las reglamentaciones penitenciarias existentes dentro de un (1) año a partir de la entrada en vigencia de la presente ley, a efectos de concordarlas con sus disposiciones. De igual forma, se invita a las provincias y a la Ciudad Autónoma de Buenos Aires a readecuar su legislación y reglamentaciones penitenciarias”.

La Provincia de Jujuy no ha dictado hasta el momento una ley de adhesión ni ha modificado su Código Procesal Penal (Ley 6.259 reformado por Ley 6.400) para receptar los cambios de la reforma efectuada por la Ley 27.375.

Este criterio ha sido compartido por diversos tribunales provinciales. Así, la Cámara de Ejecución Penal de la Provincia de Córdoba, en autos *M., J. A. s/ Libertad condicional* (Resolución N.º 112, 12/11/2019), sostuvo que las disposiciones de la Ley 27.375 “no resultan aplicables automáticamente en el ámbito provincial, por tratarse de normas de naturaleza procesal que exigen adhesión legislativa expresa”. En ese fallo, el tribunal rechazó un planteo del Ministerio Público Fiscal que pretendía aplicar el artículo 11 bis para exigir la intervención formal de la víctima en una audiencia de semilibertad, argumentando que “la regulación procesal de la ejecución penal es competencia local y no puede ser alterada por una ley nacional sin violar el principio de autonomía provincial”.

Desde una perspectiva de control de convencionalidad, este enfoque resulta adecuado. Si bien la Ley 27.375 no rige formalmente en Jujuy, sus disposiciones pueden operar como parámetros interpretativos orientados a fortalecer la tutela judicial efectiva de la víctima, en armonía con los tratados internacionales de jerarquía constitucional (art. 75 inc. 22 CN).

En síntesis, el artículo 11 bis de la Ley 24.660 reformada por la Ley 27.375, no es de aplicación obligatoria en la Provincia de Jujuy por su carácter procedimental y la ausencia de adhesión legislativa. No obstante, sus principios resultan materialmente operativos como guía de interpretación judicial conforme al bloque de constitucionalidad federal, permitiendo a los jueces locales compatibilizar la autonomía procesal con los estándares internacionales de protección de la víctima.

4.4. Jurisprudencia relevante y pautas interpretativas

La Corte Interamericana de Derechos Humanos, en *Bulacio vs. Argentina* (2003), afirmó que las víctimas y sus familiares deben tener “pleno acceso y capacidad de actuar” durante todo el proceso penal. Sin embargo, la Corte no extendió expresamente esta facultad a la etapa de ejecución en términos probatorios, sino como derecho a ser oídas y a recibir protección. De manera concordante, en *González Lluy vs. Ecuador* (2015), el tribunal interamericano estableció que la víctima tiene derecho a participar en los procesos que la afecten,

pero que dicha participación no puede traducirse en un poder de decisión que desplace las garantías judiciales del imputado o condenado.

A nivel nacional, la jurisprudencia provincial muestra distintas posiciones. Algunos tribunales, como la Cámara de Ejecución Penal de Córdoba (res. 112/2019), han admitido la participación de la víctima para ofrecer informes que acrediten riesgos, sin reconocerle facultad probatoria plena. En otras jurisdicciones, como Buenos Aires o Mendoza, se ha interpretado que la víctima puede ser oída, pero no proponer peritos ni impugnar decisiones técnicas del juez. Este criterio armoniza con la doctrina del “núcleo duro del debido proceso”, que impide que la intervención de la víctima modifique la naturaleza jurídica de la audiencia de ejecución, pero exige que el juez valore activamente la información que aporte para dictar medidas protectorias.

5. Conclusiones

El conflicto entre la tutela efectiva de la víctima y las garantías del debido proceso del condenado en la etapa de ejecución penal, exige un abordaje que combine técnica jurídica, sensibilidad institucional y equilibrio constitucional. En la práctica judicial, las audiencias de libertad condicional no pueden convertirse en escenarios de confrontación entre víctima y condenado. Su finalidad –controlar el cumplimiento de los requisitos legales y asegurar la reinserción social–, debe mantenerse como eje rector del sistema de ejecución. Sin embargo, esta finalidad no excluye el deber de proteger a la víctima. Por el contrario, impone al juez y a los operadores judiciales un rol activo de tutela, procurando que el otorgamiento de beneficios no reproduzca el daño o genere nuevos riesgos.

Desde una visión práctica, se propone distinguir claramente dos planos de actuación:

- 1) El plano técnico de la libertad condicional, donde el juez verifica objetivamente los requisitos legales, escuchando a la defensa, al Ministerio Público Fiscal y al Servicio Penitenciario.
- 2) El plano tutelar y de prevención de riesgos, donde la víctima y el Centro de Asistencia a la Víctima pueden intervenir para aportar información relevante sobre su situación de vulnerabilidad o riesgo concreto, sin alterar la naturaleza técnica del proceso.

En este segundo plano, resulta clave la actuación coordinada del Ministerio Público Fiscal, como garante de la legalidad y protector del interés público, promoviendo medidas que compatibilicen el derecho del condenado a la libertad condicional, con el derecho de la víctima a vivir sin amenazas, ni revictimización.

Los abogados litigantes, tanto de la defensa como de la querella, deben contribuir a la racionalidad del proceso: los defensores, evitando prácticas dilatorias o argumentaciones que desconozcan el deber de reinserción social del condenado; y los querellantes, canalizando los reclamos de la víctima a través de vías que fortalezcan su protección efectiva, sin interferir con la ejecución técnica de la pena.

Por su parte, los jueces de ejecución penal deben mantener el equilibrio entre ambos intereses: reconocer a la víctima un espacio real de participación, pero sin convertir la audiencia en una nueva instancia de juicio. Ello implica recibir sus manifestaciones, ponderarlas en el marco del artículo 132 del CPP de Jujuy, y disponer medidas de seguridad específicas, como prohibiciones de acercamiento, perímetros de exclusión o dispositivos de monitoreo electrónico, cuando corresponda.

Finalmente, la práctica judicial muestra que la coordinación interinstitucional entre el Juzgado de Ejecución, el Centro de Asistencia a la Víctima, el Ministerio Público Fiscal, el Ministerio Público de la Defensa Penal y los abogados litigantes, es esencial para que el sistema funcione de manera eficiente. Solo a través de este trabajo articulado se logra compatibilizar el derecho del condenado a la resocialización, con el derecho de la víctima a la protección integral, en un marco de justicia restaurativa y respeto por la dignidad humana.

En síntesis, la solución no reside en ampliar o restringir derechos, sino en interpretarlos de manera armónica y proporcional, asegurando que la ejecución penal cumpla su doble función: proteger a la sociedad y garantizar la reinserción social del condenado, sin desatender la voz ni la seguridad de quienes padecieron el delito.

Referencias

- Binder, A. M. (2013). *Introducción al derecho procesal penal*. Ad-Hoc.
- Bovino, A. (2015). *Derechos humanos y proceso penal*. Editores del Puerto.
- Caso *Bustos, Juan Carlos s/ recurso de casación*, 339:456 (Corte Suprema de Justicia de la Nación. 2016).
- Caso *Bulacio vs. Argentina* (Corte Interamericana de Derechos Humanos, 18 de septiembre de 2003). Obtenido de: https://www.corteidh.or.cr/docs/casos/articulos/seriec_100_esp.pdf
- Caso *González Lluy vs. Ecuador* (Corte Interamericana de Derechos Humanos, 1º de septiembre de 2015). Obtenido de: https://www.corteidh.or.cr/docs/casos/articulos/seriec_298_esp.pdf
- Caso *González y otras "Campo Algodonero" vs. México* (Corte Interamericana de Derechos Humanos, 16 de noviembre de 2009): https://www.corteidh.or.cr/docs/casos/articulos/seriec_205_esp.pdf
- Caso *R., G. F. s/ Ejecución de la Pena*, Expte. No. 48.234/2020 (Cámara Primera del Crimen de Mendoza, 10 de septiembre de 2020).
- Donna, E. A. (2019). *Derecho penal. Parte general* (4.^a ed.). Rubinzal-Culzoni.
- Maier, J. E. (2004). *Derecho procesal penal*. Tomo I. Hammurabi.
- Tiffer, C. (2020). *Manual de ejecución penal y derechos humanos*. IIDH.
- Zaffaroni, E. R. (2011). *Derecho penal. Parte general* (2.^a ed.). Ediar.

LAS PERSONAS VULNERABLES Y LA BRECHA DIGITAL

Vulnerable People and the Digital Divide

Víctor Rubén Colina* y María Eugenia Soza**

Univ. Católica de Salta / Univ. Católica de Santiago del Estero

rubencolina9@hotmail.com / meugeniasoza@gmail.com

RECIBIDO 23/10/2025 - ACEPTADO 17/11/2025

Resumen

El artículo analiza la brecha digital como fenómeno multifactorial que reproduce desigualdades estructurales y profundiza la vulnerabilidad de grupos desfavorecidos. Sostiene que la brecha excede el acceso a dispositivos o conectividad, e incluye competencias y capacidad de uso efectivo de las TIC. Destaca el carácter habilitante del acceso a internet para otros derechos y revisa los marcos normativos vigentes. Presenta a la Provincia de Jujuy como caso innovador por reconocer derechos digitales en su Constitución de 2023 y concluye que su efectividad exige políticas sostenidas, infraestructura y alfabetización digital enfocadas en los sectores más vulnerables.

Palabras clave:

brecha digital, vulnerabilidad, derechos humanos, competencias digitales, inclusión digital.

Abstract

The article examines the digital divide as a multidimensional phenomenon that reproduces structural inequalities and deepens the vulnerability of disadvantaged groups. It argues that the divide goes beyond access to devices or connectivity and includes the skills and effective capacity to use ICTs. It underscores the enabling nature of internet access for other rights and reviews existing regulatory frameworks. The Province of Jujuy is presented as an innovative case for recognizing digital rights in its 2023 Constitution. The article concludes that their effectiveness requires sustained public policies focused on the most vulnerable sectors.

Keywords:

digital divide, vulnerability, human rights, digital skills, digital inclusion.

1. Introducción

En un mundo en el que cada día avanza más el uso de las herramientas tecnológicas y en el que la tecnología es transversal a casi todas las actividades cotidianas de la vida de la mayoría de las personas, es preciso reflexionar sobre la brecha digital, y cómo esta desigualdad afecta a las personas en condiciones de vulnerabilidad a lo largo del planeta.

Hemos de partir formulando un cuestionamiento, ¿es el acceso al uso de internet y a las tecnologías de la información y la comunicación (en adelante, TIC) un derecho humano?

* Abogado. Escribano. Profesor en Ciencias Jurídicas. Especialista en Derecho Penal, Derechos Procesal Civil y Justicia Constitucional y Derechos Humanos. Magister en Justicia Constitucional y Derechos Humanos.

** Abogada, Especialista en Derecho Procesal, Justicia Constitucional y Derechos Humanos con orientación en minorías. Magister en Justicia Constitucional y Derechos Humanos.

La respuesta positiva surge, para nosotros, con meridiana claridad. Ahora bien, ¿cuál es el alcance de este derecho con respecto a las personas en situación de vulnerabilidad?

Se hace preciso pensar la normativa que nos rige, sobre todo en un mundo en el que las fronteras parecieran diluirse con la globalización, y que remarca las grandes diferencias y exclusiones que padecen algunos grupos de personas que se encuentran en situación de vulnerabilidad. Frente a las diversas desventajas que ciertos colectivos padecen para hacer realidad sus derechos, acaso la brecha digital se convierta en un nuevo escollo que aleje a las personas de la tutela efectiva de sus derechos.

En este artículo se realizará un análisis respecto a cuáles son algunos de los datos relevantes actuales sobre el uso de TIC en el mundo, cuál es el alcance de la brecha digital y qué iniciativas se han planteado para reducir esta brecha tanto a nivel global como en nuestro país. Por último, se abordará la normativa de nuestra provincia (Jujuy), que se encuentra a la palestra en materia constitucional, considerando las disposiciones del capítulo quinto de la nueva constitución provincial.

2. Conceptualizando la brecha digital

El origen del término “brecha digital” es incierto. Sin embargo, publicaciones recientes dan cuenta de que este concepto fue utilizado por primera vez a mediados de la década de los noventa en un reporte oficial por la Administración Nacional de Información y Telecomunicaciones del Departamento de Comercio de los Estados Unidos (Gunkel, 2003).

En un principio, el concepto hacía referencia a la desigualdad entre aquellos que tenían o no acceso físico a las TIC, pero con la evolución de la tecnología y el avance de la globalización, este concepto fue ampliándose. Así, Pipa Norris (2021) postula que no se puede hablar de un solo tipo de brecha, más bien plantea la existencia de distintos tipos de brecha: en primer lugar, la brecha social, que se enfoca en la diferencia en el acceso a la información entre los pobres y ricos en cada país; en segundo lugar, la brecha global, que es la diferencia entre países desarrollados y en desarrollo en el uso de TIC; y, por último, la brecha democrática, como la diferencia entre quienes utilizan las TIC para movilizarse y participar en la esfera pública de quienes no poseen ni el acceso ni las habilidades que la tecnología requiere para su aprovechamiento.

En la actualidad, no existen dudas de que la brecha digital es paralela a las divisiones económicas, raciales y de género que atraviesan a la sociedad. Estas diferencias comprenden tanto la desigualdad en el acceso a nuevas tecnologías como la falta de conocimiento sobre su uso y potencial en los casos en que la tecnología es accesible. Es decir, cuando hablamos de brecha digital no solo hablamos del acceso a la tecnología, sino también de la falta o insuficiencia de habilidades necesarias para su uso. En otras palabras, nos referimos a las competencias digitales.

La continua evolución de las TIC ha provocado progresivamente en las personas la necesidad de adquirir niveles cada vez más altos de alfabetización digital para mantener su sentido de inclusión, lo que sin dudas ha causado que una gran porción de la población se sienta excluida de las ventajas que acarrea el uso de las nuevas tecnologías. Un claro ejemplo se puede encontrar en los adultos mayores que ven como inaccesibles tareas que otrora

fueran sencillas, como el pago de servicios, el transporte público, o trámites administrativos.

Se ha señalado que la brecha se manifiesta no solo en la disponibilidad de recursos tecnológicos, sino también en las competencias asociadas a su uso y utilidad (Gutiérrez-Provecho *et al.*, 2021). Estos autores proponen que la superación de esta brecha requiere no sólo la adquisición de infraestructura, sino también la motivación y formación en su uso y apropiación. Su investigación evidencia la existencia de una brecha digital significativa tanto de acceso (disponibilidad de tecnología) como de uso (utilización para búsqueda de empleo y trámites administrativos), particularmente en poblaciones vulnerables.

En síntesis, podemos colegir que la brecha digital en estos tiempos es un fenómeno multifactorial, que se refiere a la desigualdad en el acceso y uso de las TIC entre individuos, grupos sociales y países. Esta desigualdad va más allá de la mera disponibilidad de recursos tecnológicos y también incluye la falta de competencias y habilidades para utilizarlos de manera efectiva.

3. Los derechos humanos y las personas en situación de vulnerabilidad

La idea de que hay derechos inherentes a los seres humanos es una noción bastante antigua. Se encuentran antecedentes en los pueblos hebreos o en la Grecia clásica, donde se hablaba de leyes no escritas o leyes naturales. Esta noción ha ido transformándose paulatinamente hasta llegar a la concepción moderna de los derechos humanos.

En el derecho positivo, los documentos que se pueden tomar como antecedentes en la tutela de los derechos humanos son la Carta Magna de 1215, el *Habeas Corpus* de 1679 y el *Bill of Rights* de 1689, en Inglaterra; también, la Declaración de Independencia de los Estados Unidos de 1776. El acontecimiento considerado como verdadero punto de partida de los derechos humanos en el sentido actual es la “Declaración de los derechos del hombre y del ciudadano”, emanada durante la Revolución Francesa en 1789. Esta declaración constituyó la fuente de las libertades contemporáneas. Con el correr del tiempo, dichas declaraciones tomaron el peso de normas fundamentales o constitucionales y las garantías individuales, contenidas en las mismas, fueron adquiriendo positividad normativa. Así, los derechos fundamentales se abrieron paso hacia su consolidación interna por medio del Derecho Constitucional, para dejar de ser utopías.

Como es sabido, por su parte, la expresión “derechos humanos” en su sentido actual es relativamente nueva y surge con el fin de la Segunda Guerra Mundial y la consecuente constitución de la Organización de las Naciones Unidas. Fue, justamente, luego de las atrocidades cometidas en esa guerra que la comunidad internacional vio la imperiosa necesidad de hacer frente a las violaciones de derechos humanos a través de instrumentos legales y mecanismos de tutela de los derechos humanos.

La Carta de las Naciones Unidas trajo como novedad la repetida mención del término “derechos humanos”; sin embargo, en la misma no surge una definición concreta. En la Declaración Universal de los Derechos Humanos y la Declaración Americana de los Derechos y Deberes del Hombre de 1948 se puede marcar el momento en que se inició el desa-

rrrollo pormenorizado de los derechos humanos y se establecieron pautas para su interpretación.

La Declaración Universal fue reforzada con los pactos de derechos humanos adoptados dentro del marco de las Naciones Unidas en 1966 y vigentes a partir de 1976. Dichos pactos son: el Pacto Internacional de Derechos Civiles y Políticos y el Pacto Internacional de Derechos Económicos, Sociales y Culturales. Ambos instrumentos definen con mayor precisión los derechos humanos, introducen importantes matices y algunas innovaciones. Además, el Pacto Internacional de Derecho Civiles y Políticos, al crear el Comité de Derechos Humanos y contemplar mecanismos de protección, constituye un importante aporte para la efectiva observancia obligatoria de dichos derechos.

Pese a estos denodados esfuerzos por construir herramientas de protección para la dignidad humana, las desigualdades siguen existiendo y las personas en determinadas condiciones se ven imposibilitadas de concretar el efectivo ejercicio de sus derechos. Esta situación ha llevado a la comunidad internacional a generar nuevos instrumentos internacionales que visibilizan la situación de las personas vulnerables por una diversidad de motivos, así como las obligaciones de los Estados frente a ellas. Así surgen, por ejemplo, las 100 Reglas de Brasilia, que formulan un análisis respecto de quiénes se consideran sujetos vulnerables, pero de este análisis queda claro que todos ellos poseen ciertos rasgos característicos.

En este orden de ideas, la Regla N° 3 define: “Se consideran en condición de vulnerabilidad aquellas personas que, por razón de su edad, género, estado físico o mental, o por circunstancias sociales, económicas, étnicas y/o culturales, encuentran especiales dificultades para ejercitar con plenitud ante el sistema de justicia los derechos reconocidos por el ordenamiento jurídico”.

Llevando adelante un estudio exhaustivo de las diversas categorías se ha dicho que: “un sujeto en condición de vulnerabilidad es aquel que debido a una cualidad intrínseca de su persona encuentra una restricción mayor que la del resto de la población para defender sus derechos, ya sea al momento de la apertura de la instancia judicial como durante la tramitación del juicio, y que por lo tanto, obliga a los operadores de justicia a aplicar las reglas del proceso de una manera activa, para que al entrar en contacto con la justicia la persona no sufra una doble vulnerabilidad, menoscabando derechos fundamentales y causando un daño irreparable” (Gutiérrez-Provecho *et al.*, 2021).

Esta situación especial de las personas “en condición de vulnerabilidad” hace que por eso mismo encuentren especiales dificultades para ejercitar con plenitud ante el sistema de justicia los derechos reconocidos por el ordenamiento jurídico. En el ámbito específico de nuestro análisis, ha de observarse que cuando estas personas deben usar las TIC, encuentran barreras, ya sea por la falta de acceso a dispositivos digitales o internet, pero también por la falta de habilidades, de experiencia o de confianza tanto como inseguridades. Es decir que, en su estudio, no se puede dejar de considerar las diferentes interseccionalidades.

En este sentido, resulta ilustrativo acudir a determinados índices globales. Por ejemplo, un informe estima que el número de usuarios de internet a nivel global alcanzará los 5.560 millones este año. Esto representa un crecimiento del 2,5% anual. A fines del 2024, aproximadamente, el 68% de la población mundial tenía acceso a una conexión a internet. Sin

embargo, la brecha de acceso sigue siendo significativa. Las regiones con la menor penetración de internet son África central (33,6%) y África oriental (42,5%). Esto contrasta con las regiones con mayor penetración, como el norte de Europa (98,8%) o Europa del Sur (91,6%). Aunque el uso de internet es cada vez más equitativo, el mismo informe señala que todavía existen diferencias: verbigracia, el 96,5% de las niñas de 10 a 15 años usan internet frente al 95,5% de los niños, pero las mujeres muestran más preocupación por la protección de datos personales, lo que señalaría la implicancia de las redes sociales en la vida de las niñas y mujeres. Se calcula que se necesitan entre 2,6 y 2,8 billones de dólares para conectar significativamente a toda la población mundial para 2030. Esta inversión se destinaría a áreas como infraestructura digital, asequibilidad de dispositivos y habilidades digitales¹.

A su vez, la Declaración de Derechos del Ciberespacio señala claramente que la brecha digital no sólo divide a ricos y pobres, sino que surge de cualquier factor que marque la diferencia entre quienes acceden a la información y quienes quedan fuera de ella, como jóvenes y mayores, hombres y mujeres, o personas en plenitud de condiciones físicas y mentales y personas con discapacidades, por lo que la accesibilidad de la información es un requisito esencial para la eliminación de la brecha digital (Suñé Llinás, 2022).

El Plan de Gestión 2022-2026 elaborado por el Centro de Estudios de Justicia de las Américas² —organismo de innegable incidencia en la región—, reconoce que el desafío para los próximos años consiste en la consolidación e integración de los nuevos procesos organizativos y recursos tecnológicos a fin de generar más eficiencia y oportunidad en los servicios judiciales, así como para reducir las brechas de acceso para las personas en situación de vulnerabilidad.

4. El acceso a internet y su evolución como derecho básico

El acceso a internet considerado como un derecho básico es una idea que resulta prácticamente incontrovertible en los tiempos modernos y que se ha traducido en diversos documentos como, por ejemplo, la Carta sobre Derechos en Internet³ (2006) de la Asociación para el Progreso de las Comunicaciones. Allí se afirma que un acceso “asequible, rápido y fácil a internet puede ayudar a generar sociedades más igualitarias”. En el apartado segundo de la Carta, se considera que internet funciona como una estructura pública global y, como tal, debe ser “ampliamente distribuida y ser soporte del ancho de banda suficiente para permitir a las personas de todas partes del mundo utilizar ese potencial para hacerse oír, mejorar su vida y expresar su creatividad”.

Algunos países iberoamericanos han avanzado en su reconocimiento mediante su admisión en sus constituciones, en una legislación específica, o bien, en forma indirecta en normas sobre temáticas vinculadas. Tal es, por ejemplo, el caso de España a través de su Ley

¹ Los datos surgen del “Digital 2025: Global Overview Report”. Cf. también el reporte de la Unión Internacional de Telecomunicaciones, disponible en: <https://www.itu.int/reports/council/>

² Para más información, cf. “Plan Estratégico del Centro de Estudios de Justicia de las Américas 2022-2026”. Disponible en: <https://cejamericas.org/plan-estrategico-2022/>

³ Disponible en: https://www.apc.org/sites/default/files/APC_charter_ES_2.pdf

Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (BOE-A-2018-16673 3/2018), la cual, en su artículo 81, reconoce que todos “tienen derecho a acceder a internet independientemente de su condición personal, social, económica o geográfica”. Algo similar ocurre en Grecia, que reconoce en su Constitución el acceso a la información electrónica (desarrollada por internet) como un derecho fundamental en la esfera de los Derechos Sociales e Individuales. La constitución griega (art. 5º, n. 2) estipula que el derecho a la información debe asegurarse para el disfrute de todos los ciudadanos en aras de participar en sociedad. Por este motivo, es una obligación del Estado facilitar el acceso a la información electrónica en sus dimensiones de producción, intercambio y difusión, con resguardo de las garantías de protección electrónica de datos personales y el secreto de comunicaciones. Encontramos disposiciones similares en países como México, Colombia, Perú, Chile y Costa Rica, entre otros.

En este orden de ideas, la Asamblea General de la Organización de las Naciones Unidas por medio de su ex Relator Especial sobre la Promoción y Protección del Derecho a la Libertad de Opinión y de Expresión, Frank La Rue, en su Informe Anual del año 2011 sostuvo que la meta del acceso universal a internet debe ser una prioridad para todos los Estados, y que “en consecuencia, cada uno debe elaborar una política eficaz y concreta, a fin de que internet resulte ampliamente disponible, accesible y asequible para todos los sectores de la población”.⁴

En la Cumbre de la ONU sobre el Desarrollo Sostenible fue aprobada la “Agenda 2030 para el Desarrollo Sostenible”, que asume un compromiso de “no dejar a nadie atrás”, esto es, empoderar a las personas vulnerables. Este documento, que el gobierno argentino hizo propio, afirma enfáticamente que “el desarrollo sostenible no puede hacerse realidad sin que haya paz y seguridad, y la paz y la seguridad corren peligro sin el desarrollo sostenible”⁵. De lo expuesto, podemos colegir que la nueva agenda global, reconoce la necesidad de construir sociedades pacíficas, justas e inclusivas que proporcionen igualdad de acceso a la justicia y se basen en el respeto de los derechos humanos (incluido el derecho al desarrollo), en un estado de derecho efectivo y una buena gobernanza a todos los niveles, y en instituciones transparentes y eficaces que rindan cuenta.

Frente a estos compromisos, lo que resta analizar es de qué manera estas normas se convierten en realidades concretas. En el territorio donde las personas se interrelacionan, donde ejercen sus derechos, se precisan acciones concretas.

5. Sobre brecha digital en Argentina

La brecha digital en Argentina, al igual que en otros países, se caracteriza por la persistencia de desigualdades en tres aspectos principales: acceso, uso y habilidades. Según el INDEC (Instituto Nacional de Estadística y Censos), al segundo trimestre de 2025, el 93,7% de los hogares urbanos tiene acceso a internet (fijo o móvil). Sin embargo, persisten grandes asimetrías regionales. Por ejemplo, mientras la Ciudad de Buenos Aires tiene una alta tasa de acceso, otras provincias como Formosa y Santiago del Estero tienen porcentajes de acceso

⁴ Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión. Consejo de Derechos Humanos, 17º período de sesiones, A/HRC/17/27.

⁵ Cf. https://www.argentina.gob.ar/sites/default/files/lenguaje_claro_web.pdf

a internet significativamente más bajos, y hasta un 17% de su población vive en hogares sin ninguna conexión.

Es relevante destacar que, hacia finales de 2024, el 60,3% de los hogares urbanos tenía acceso a una computadora. Sin embargo, una gran parte de la población se conecta a internet principalmente a través de teléfonos celulares. Esto genera una brecha educativa, ya que la mayoría de los estudiantes se conecta desde telefonía móvil lo que es inadecuado para realizar tareas educativas o de aprendizaje que requieren procesadores de texto o software de creación, lo que se hizo más visible durante la pandemia de Covid-19, cuando no solo las familias debían adaptarse a las clases virtuales, sino que muchas de ellas solo contaban con un medio de conexión y varios de sus miembros que precisaban de dichos elementos.

Para reducir la brecha digital se han articulado programas como Conectar Igualdad, que fue una iniciativa del Ministerio de Educación que buscaba reducir la brecha digital en las escuelas públicas a través de la entrega de netbooks a estudiantes y docentes, y la provisión de recursos y capacitación tecnológica. Su objetivo principal era garantizar el acceso a la tecnología y mejorar la calidad educativa en todos los niveles. Fue una de las políticas de inclusión digital más importantes del país. Aunque tuvo un impacto positivo en la reducción de la brecha de acceso, el programa fue discontinuado.

Otra iniciativa que tuvo el estado argentino fue la Red Federal de Fibra Óptica (REFEFO), una acción del gobierno para expandir la conectividad de banda ancha a lo largo del país, especialmente en áreas donde los operadores privados no llegan por falta de rentabilidad. También se habilitaron más de 420 Puntos Digitales en todo el país, los cuales eran espacios públicos con acceso gratuito a computadoras e internet, y a partir de los cuales se ofrecía capacitaciones en alfabetización digital para la comunidad.

En el ámbito del derecho, en el año 2014 se promulgó la Ley 27.078 “Argentina Digital”, cuyo objetivo inicial fue promover el interés público en el desarrollo de TIC, la neutralidad de las redes, entre otras regulaciones y sus recursos asociados. Esta ley llegó como un necesario reemplazo, aunque algo deficiente, de la obsoleta ley de telecomunicaciones de 1972, pero adolece de algunas vaguedades conceptuales y cierta ambigüedad, ya que regula no sólo telecomunicaciones, sino también servicios de internet e incluso redes privadas, lo que podría ser un avance sobre la libertad de expresión y la innovación. La norma ha sido ampliamente criticada por otorgarle al ENACOM (Ente Nacional de Comunicaciones) excesivos poderes discrecionales de control, entre otras críticas que se han sostenido en el tiempo.

Sin embargo, como normativa es un avance que debe ser tenido en cuenta, ya que esta ley declara de interés público las TIC y la neutralidad de las redes, con el objetivo de garantizar el acceso universal a los servicios de información y comunicación en condiciones equitativas y de alta calidad. Esta ley también tiene como aporte positivo normas que establecen los derechos de los usuarios y promueve la competencia en los servicios.

6. El caso de la Provincia de Jujuy

El 21 de junio de 2023, la Provincia de Jujuy aprobó una nueva Constitución Provincial. Entre los cambios relevantes que trajo esta reforma que incorpora el capítulo Quinto, referente a nuevas declaraciones, derechos, deberes y garantías constitucionales, desde el art. 72 al 77, se incorporan nuevos derechos vinculados al acceso a internet, lo que posiciona a esta normativa en un punto de referencia en relación a los derechos digitales.

En el art. 72 se hace referencia a la democratización del conocimiento, poniendo en cabeza del Estado estas arduas tareas, promoviendo la conectividad universal y efectiva como un medio para garantizar la igualdad de oportunidades y el ejercicio de los derechos, así como también promover el acceso a las TIC, en condiciones de igualdad, accesibilidad y asequibilidad para todas las personas y promover políticas públicas de inclusión digital procurando el acceso de las personas a las herramientas y recursos tecnológicos necesarios para participar plenamente en la vida social, política, económica, productiva y cultural de la provincia. Hemos de destacar lo ambicioso del contenido propuesto por los constituyentes, toda vez que la concreción de esta norma requiere una gran inversión en infraestructura y recursos.

Por su parte, el art. 73 de manera clara y contundente establece el derecho de todas las personas al acceso a la innovación y la tecnología en todas sus formas, así como a intervenir y participar de su producción, respetando los derechos, principios y garantías fundamentales consagradas por la Constitución. Es este un avance para reducir la brecha digital, por cuanto se pone en cabeza del Estado la promoción de la innovación y el desarrollo científico y tecnológico en todos sus campos, reconociendo el derecho de todas las personas a la educación en tecnología e innovación, herramienta fundamental para garantizar el acceso y el aprovechamiento de la tecnología en beneficio propio y de la sociedad. Sin embargo, se establece como límite el respeto de los derechos humanos y los principios éticos que establezca la ley. Siguiendo ese orden de ideas, por su parte el art. 74 se refiere a la producción de bienes y servicios biotecnológicos, haciendo la salvedad de los casos en los que se produzca conflicto entre los derechos humanos y el desarrollo, producción o uso de herramientas biotecnológicas, sosteniendo la primacía de los derechos humanos.

En relación al acceso a nuevas tecnologías, el art. 75 dispone que todas las personas tienen derecho a decidir libremente sobre el uso o acceso a dispositivos tecnológicos que interactúen con procesos biológicos para mejorar su salud y calidad de vida, en tanto no atenten contra su integridad física, psicológica y moral, ni la de otros seres humanos. Y frente a este derecho, en el segundo inciso se dispone la obligación del Estado de promover la igualdad de acceso a estas mejoras, sin discriminación alguna y en concordancia con estándares internacionales de protección de los derechos humanos.

Avanzando un paso más en estas innovaciones, el art. 76 se refiere al reconocimiento del derecho de las personas al uso de sistemas de inteligencia artificial o no humana, basados en métodos computarizados de algoritmos, datos y modelos que imitan el comportamiento humano y automatizan procesos complejos, así como otros futuros desarrollos que surjan en este campo. Este derecho se fundamenta en los principios de legalidad, transparencia, responsabilidad, privacidad y protección de datos, seguridad, no discrimi-

nación y rendición de cuentas, garantizando el acceso a la justicia en caso de vulneración de derechos y consagrando la acción de solicitud de revisión humana cuando sea necesario.

En el artículo aludido, se incluye el deber del Estado de fomentar la investigación y el desarrollo de estos sistemas en beneficio de la población, la educación y el debate público sobre los desafíos éticos y jurídicos que plantean estos sistemas, incluyendo sus efectos sobre la transformación del mundo laboral. Se reitera la premisa, para los casos de conflicto de derechos a partir del uso de estos sistemas, de aplicar el principio de primacía de los derechos humanos y de las libertades y garantías constitucionales a favor de las personas. Es evidente que, en estos artículos antes mencionados, los constituyentes han plasmado el principio de progresividad de los derechos humanos, por cuanto los mismos implican un avance en su reconocimiento, sin que esto implique una disminución o reducción de los ya reconocidos, siendo el bien común el fin último de esta normativa.

Por último, en esta secuencia normativa, el artículo 77 establece el derecho a la protección de los datos personales y la acción de *habeas data*, en correlato con la Constitución Nacional.

Estas normas representan un gran avance, pero implican también un gran desafío y responsabilidad para el Estado Provincial. En el marco de una sociedad que evoluciona constantemente, se hace necesario generar normas que puedan reglamentar y concretizar el ejercicio de estos nuevos derechos y deberes, pero más allá de la norma se necesita voluntad, compromiso y planificación que descienda a la realidad la letra constitucional. Este compromiso requiere de la creación de espacios y programas cuyo objetivo sea reducir la brecha digital que sufren en particular los sujetos en condiciones de vulnerabilidad, para que el acceso a la tecnología, el aprendizaje y la incorporación de habilidades sean políticas perdurables con independencia de los sujetos que ostenten cargos y funciones públicas.

7. Conclusiones

Por todo lo antes dicho podemos afirmar con solvencia que la brecha digital es multifactorial y refleja desigualdades estructurales. No se limita al acceso físico a internet o dispositivos, sino que también abarca las desigualdades en las habilidades, la motivación y la capacidad para utilizar las TIC de manera efectiva. Esta brecha es paralela a las divisiones económicas, sociales, de género, etarias y raciales preexistentes.

Las personas en situación de vulnerabilidad son las más afectadas, pues son quienes ya enfrentan barreras para ejercer sus derechos (por edad, género, condición socioeconómica, ubicación geográfica, etc.) y encuentran obstáculos adicionales en el entorno digital, lo que profundiza su exclusión y genera una “doble vulnerabilidad”.

El acceso a internet es un derecho humano fundamental, y en tal sentido existe un consenso internacional y un avance normativo creciente que reconoce el acceso universal, asequible y de calidad a internet como un derecho habilitante para el ejercicio de otros derechos, como la educación, la salud, la participación y la libertad de expresión. Pero, a pesar de los marcos legales generados en distintos países y los compromisos internacionales (como la Agenda 2030), persisten grandes desafíos para materializar estos derechos ya consagrados,

especialmente en regiones con menor desarrollo y en poblaciones vulnerables, donde la brecha de acceso a las nuevas tecnologías sigue siendo significativa.

Nuestro país ha tenido un devenir histórico con avances y retrocesos en la reducción de esta brecha. Si bien existen políticas históricas de inclusión digital como Conectar Igualdad y la Red Federal de Fibra Óptica, estas han sido discontinuadas, lo que evidencia una falta de prioridad en la agenda pública.

La Provincia de Jujuy se destaca como un caso de vanguardia normativa. Su reforma constitucional de 2023 consagra explícitamente derechos digitales innovadores, como el acceso a la tecnología, la innovación, la protección de datos frente a sistemas de inteligencia artificial y la obligación del Estado de promover la inclusión digital. Esto representa un modelo a seguir, pero también un desafío en su implementación.

De lo ya expuesto, podemos colegir que la educación y la capacitación son pilares fundamentales para el adecuado uso de las nuevas tecnologías. Superar la brecha digital requiere no solo de infraestructura, sino también de políticas públicas sostenidas de alfabetización digital que empoderen a los ciudadanos, especialmente a los más vulnerables, para utilizar la tecnología en su beneficio.

En pocas palabras, se necesita voluntad política, planificación y estabilidad. Además del reconocimiento normativo, se requiere un compromiso firme sobre la continuidad de los programas de inclusión y una planificación estratégica para que los derechos reconocidos formalmente se conviertan en realidades tangibles para toda la población, priorizando a los grupos en situación de vulnerabilidad.

Referencias

- Asociación para el Progreso de las Comunicaciones (APC). (2006). Carta sobre Der. en Internet. Disponible en: https://www.apc.org/sites/default/files/APC_charter_ES_2.pdf
- Gunkel, D.J. (2003). "Second thoughts: toward a critique of the digital divide". *New Media & Society*, 5(4), 499-522. Recuperado de: http://www.gunkelweb.com/articles/digital_divide.pdf
- Gutiérrez-Provecho, M. L., López-Aguado, M., García LLamas, J. L., & Quintanal Díaz, J. (2021). La brecha digital en población en riesgo de exclusión social. *Pedagogía Social Revista Interuniversitaria*, (39), en: https://doi.org/10.7179/PSRI_2021.39.08
- La Rue, F. (2011). Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión. Consejo de Derechos Humanos, 17º período de sesiones, A/HRC/17/27.
- Norris, P. (2001). *Digital Divide, Civic Engagement, Information Poverty and the Internet Worldwide*. Cambridge: Cambridge University Press.
- ONU (2015). Agenda 2030 para el desarrollo Sostenible. Asamblea General de las Naciones Unidas. Disponible en: https://www.argentina.gob.ar/sites/default/files/lenguaje_claro_web.pdf
- Portal de la Unión Internacional de Telecomunicaciones (2021). 2.900 millones de personas siguen careciendo de conexión: <https://www.itu.int/es/mediacentre/Pages/PR-2021-11-29-FactsFigures.aspx>
- Suñé Llinás, E. (2022). "Derechos humanos en el ciberespacio", *Biblioteca digital de difusión científica de la Universidad Veracruzana México*, disponible en: <https://www.uv.mx/mdhjc/files/2022/01/Derechos-Humanos-en-el-Ciberespacio.pdf>

LA INVESTIGACIÓN CRIMINAL EN BASE AL ANÁLISIS DE LAS COMUNICACIONES: UN MÉTODO

Criminal Investigation Based on Communications Analysis: A Method

Maximiliano Rubén Gomez* y Francisco Brocca**

Universidad Nacional del Oeste

mrgomez@mpba.gov.ar / fbrocca@uno.edu.ar

RECIBIDO 06/11/2025 - ACEPTADO 17/11/2025

Resumen

La evolución constante de las modalidades delictivas exige adaptar las herramientas tecnológicas aplicadas a la investigación penal. En este contexto, el análisis de comunicaciones puede resultar determinante para establecer la intervención y autoría en hechos ilícitos, aunque su complejidad técnica dificulta su comprensión y valoración probatoria. Por ello, se vuelve esencial contar con un método de investigación claro y estructurado que asista a analistas y operadores del sistema penal.

Palabras clave:

Método, análisis de las comunicaciones telefónicas, investigación, garantías constitucionales.

Abstract

The constant evolution of criminal modalities demands the adaptation of technological tools used in criminal investigations. Communication analysis can be decisive in establishing involvement and authorship in unlawful acts, although its technical complexity hinders both understanding and evidentiary assessment. Therefore, a clear and structured investigative method becomes essential to support analysts and practitioners within the criminal justice system.

Keywords:

method, communication analysis, investigation, constitutional rights.

1. Introducción

En los tiempos actuales el acceso a las nuevas tecnologías de comunicación pone de manifiesto el avance de un cambio de paradigma, sobre todo en el aspecto de la investigación

* Ayudante Fiscal U.F.I Nro. 7 de MGR. Abogado con distinción de diploma de honor (UBA). Especialista en Derecho penal y en Litigio Penal (UBA). Diplomado en Sistema Penal y Nuevas modalidades delictivas, en Derecho Constitucional y Magistratura y en Derechos Humanos control de Convencionalidad y Constitucionalidad Universidad Nacional del Oeste. (UNO). Ayudante docente en Teoría del Delito (UBA). Profesor de IUNMA en Derecho Penal Parte Especial. Profesor de Estado y Sociedad, Política Criminal y del Seminario de gestión Policial-Judicial del (IUV). Profesor de las materias Derecho Penal I, Derecho Procesal Penal, Derecho Penal Parte Especial y Taller de investigación Criminal I y II de la Tecnicatura Universitaria en Investigación Criminal (UNO). Director de la Diplomatura Universitaria en Investigación Criminal (UNDELTA). Investigador de la Universidad Nacional del Oeste.

** Secretario de la U.F.I. Nro. 1 de Trenque Lauquen. Abogado de la Universidad de Buenos Aires (UBA). Diplomado en Sistema Penal y Nuevas modalidades delictivas; en Derecho Constitucional y Magistratura; y en Derechos Humanos control de convencionalidad y constitucionalidad; todas de la Universidad Nacional del Oeste. (UNO). Ayudante docente en Derecho Internacional Público (UBA, 2017-2023). Jefe de Trabajos Prácticos en Derecho Internacional Público (Universidad Dr. Plácido Marín, 2021-2023). Profesor de las materias Derecho Procesal Penal, Investigación y Derechos Humanos y Taller de Investigación Criminal 1 de la Tecnicatura Universitaria en Investigación Criminal (UNO).

criminal. Algo tan simple como un teléfono celular inteligente nos permite comunicarnos con personas a miles de kilómetros de distancia, a través de mensajes multimedia, navegación en internet, y el registro de sus ubicaciones, entre tantas otras cosas.

En otras palabras, las nuevas tecnologías han cambiado la forma de relacionarse entre las personas. Sin embargo, no todo es color de rosa. Estas tecnologías han provocado una expansión en el ámbito jurídico penal, no sólo en las investigaciones, sino que han proliferado nuevas modalidades delictivas digitales (defraudaciones informáticas, *grooming*, robo de datos, etc.). En tal sentido, estas nuevas herramientas son utilizadas para el funcionamiento de bandas criminales, las cuales han ido perfeccionando su uso para la comisión o encubrimiento de delitos. En contrapartida, el análisis de los teléfonos celulares de los imputados se vuelve un elemento clave en la investigación, como así el estudio de toda la evidencia digital que él contenga.

Intentaremos, a lo largo del presente artículo, establecer cómo una de las aristas de la evidencia digital, las telecomunicaciones, se impone como de vital interés para las investigaciones criminales. Además, propondremos un método de investigación para su análisis que podría resultar superador para la eficiencia investigativa.

2. El análisis de las comunicaciones

Si bien el objetivo central del presente es el análisis de las telecomunicaciones, no podemos pasar por alto el concepto de evidencia digital y sus diversas acepciones. En tal sentido, como primera aproximación podemos definir la evidencia digital como cualquier información sujeta a una intervención humana, electrónica y/o informática que ha sido extraída de un medio tecnológico informático; por ejemplo: computadoras, celulares, aparatos digitales, medios ópticos. Técnicamente es un tipo de evidencia física que puede ser recolectada y analizada con herramientas y técnicas especiales (Ministerio de Seguridad de la Nación, 2023, p. 5).

En consecuencia, podemos decir que la evidencia digital es todo dato o conjunto de datos informáticos introducidos en un proceso con fines probatorios, que pueda provenir de archivos, registros, mensajes electrónicos, registros de actividad en línea, metadatos, imágenes, y cualquier otro dato almacenado en dispositivos electrónicos o sistemas informáticos (“Protocolo de gestión de almacenamiento de la evidencia digital”, MPF de CABA, 2013, p. 2). Al ser el análisis de la evidencia digital una pieza importante para el esclarecimiento de los delitos, así como para determinar el grado de participación de las personas imputadas, resulta primordial que la obtención de dichos indicios se haga respetando todas las garantías que rigen el proceso penal.

La discusión posee relevancia directa en el ámbito de injerencia sobre diferentes derechos consagrados tanto nacional como internacionalmente. Tal es así que no sólo pueden verse afectadas garantías constitucionales que rigen en el proceso penal a nivel nacional (arts. 18, 19 y 33 de la Constitución Nacional), sino también toda la normativa internacional existente al respecto, como ser el art. 11 incisos 2 y 3 de la Convención Americana sobre Derechos Humanos, art. 17 del Pacto Internacional de los Derechos Civiles y Políticos, art. 12 de la Declaración Universal de Derechos Humanos y 10 de la Declaración Americana sobre Derechos Humanos.

Dichos artículos, conforman el plexo normativo que funciona como escudo contra la interceptación de las comunicaciones y la protección del ámbito de privacidad de todas las personas, sin distinción alguna. Nuestra Constitución establece particularmente al respecto que sólo una orden emitida por un juez o una ley que así lo dictamine, podrá hacer cesar este escudo de inviolabilidad de las comunicaciones, que es lo que sucede, por ejemplo, con la Ley Nacional de Telecomunicaciones o el Código Procesal Penal de la Provincia de Jujuy.

En ese camino, y en relación al punto central del análisis de las comunicaciones, el Código Procesal Penal de la Provincia de Jujuy, en su artículo 231, establece que las empresas que brinden el servicio de comunicación deberán posibilitar el cumplimiento inmediato de la diligencia, bajo apercibimiento de incurrir en responsabilidad penal y ser pasible de la imposición de multas a favor del Ministerio Público de la Acusación conforme la reglamentación que se dicte al efecto.

Este artículo evidenciaría que es el Ministerio Público Fiscal quien puede —y debe— solicitar la información de las comunicaciones telefónicas de los investigados, estableciendo que las compañías deberán facilitarle la información. A diferencia de ello, el articulado del Código Procesal Penal de la Provincia de Buenos Aires no especifica quién debe realizar el pedido de información de las telecomunicaciones. Por ello es que, resulta propicio destacar lo expuesto por los jueces la Sala I del Tribunal de Casación Penal de la Provincia de Buenos Aires en la sentencia número 68962 “L.M.A s/Recurso de Casación”.

En dicho veredicto, en primer lugar, se pone de manifiesto que el ordenamiento procesal de la provincia de Buenos Aires, no requiere —bajo pena de nulidad— la orden del juez para obtener el listado de llamadas registradas por una línea telefónica, a diferencia de lo que ocurre con la interceptación de las comunicaciones para impedir las o conocerlas (art. 229 del CPP).

Por el mismo camino, se evidencia en el precedente que, si bien la Ley Nacional de Telecomunicaciones 19.798 establece que la inviolabilidad de la correspondencia de las comunicaciones comprende tanto la “existencia” como el “contenido”, hace una diferenciación entre la autoridad que puede disponer la intervención de una comunicación, y aquella facultada para obtener los registros de tráfico de una línea telefónica.

En el caso de la intervención de su contenido, el art. 18 ordena que sólo procederá a requerimiento de juez competente, mientras que al referirse a los registros de tráfico de comunicaciones (existencia) dispone que los prestadores del servicio deberán sistematizar tal información para su consulta sin cargo por parte del Poder Judicial o el Ministerio Público, conforme el art. 45 ter incorporado por la ley 25.873 (Tribunal de la Casación Penal de la Provincia de Buenos Aires, causa número 68962 “L.M.A s/Recurso de Casación”, voto del Dr. Carral, págs. 4-6).

En relación a la influencia que este tipo de tecnología posee en la esfera privada, Diego Fernández especifica que los datos que se pueden recolectar a través de dispositivos móviles resultan extremadamente valiosos en el marco de las investigaciones judiciales, sobre todo en el marco de investigaciones y juicios penales. Pueden ayudar a establecer que un

determinado sospechoso se encontraba en el lugar donde se cometió un delito mientras este sucedía y, por tanto, resulta razonable que las autoridades tengan un interés válido en querer acceder a estos datos. En tales casos, la cuestión radica entonces en determinar cómo debe balancearse el derecho a la privacidad de los individuos frente al acceso de las autoridades a sus datos y qué resulta razonable exigir para que este acceso sea legítimo. La privacidad es el derecho que todas las personas tienen a ser dejadas solas, sin intromisión de terceros, incluyendo al Estado, sin su voluntad y consentimiento. Por supuesto, este derecho no es absoluto y existen supuestos en los que otros derechos priman sobre el derecho individual a la privacidad (Fernández, 2023, p. 816).

Habiéndose puesto en discusión cuales son los requisitos para obtener la información que será objeto del análisis de las comunicaciones, como especie de la evidencia digital, debemos aclarar que en esta oportunidad no nos centraremos en lo que generalmente acaece en un estadio más avanzado de la investigación, esto es las escuchas telefónicas (contenido). En este caso, el quid de la cuestión versará sobre el análisis de los registros (existencia) respecto de llamadas entrantes y salientes, informes GPRS o megadatos, apertura de celdas e impactos de abonados en IMEI, entre otras cuestiones.

Es importante enmarcar el objeto de estudio del análisis de las comunicaciones, pudiendo precisar que los movimientos de telecomunicaciones resultan de interés en materia de investigación criminal en razón de tres puntos de estudio. En primer lugar, el relacional, en referencia a la vinculación los abonados entre sí. En segundo término, el espacial, tendiente a la geolocalización de comunicaciones mediante el impacto en celdas telefónicas. Por último, el temporal, en pos del examen de las variables dinámicas de las comunicaciones como ser fecha y hora o duración (Martínez, 2020, p. 6).

Como se observará en lo subsiguiente, toda esa información aporta una herramienta incommensurable para las investigaciones penales. Pero antes de dar paso al método de investigación aquí propuesto, debemos definir a continuación algunos conceptos básicos para poder proseguir:

- 1) *Número de abonado*: es el número asignado desde el cual se emiten las comunicaciones (Enacom, 2011).
- 2) *Nro. de IMEI*: es el número que identifica al equipo de telefonía celular, siempre consta de 15 número, pero los 14 primeros son los que identifican al equipo, y el último es asignado por la compañía prestataria (Enacom, 2016).
- 3) *Celdas*: la celda es el espacio de cobertura de una antena de telefonía celular. Las compañías telefónicas tienen conocimiento de la ubicación exacta de las antenas, identifican el lugar donde se sitúan en función de variables de latitud y longitud. Por lo tanto, para el estudio de si el usuario de un abonado se encontró en determinado lugar será de interés: 1) lugar certero donde se ubica la antena, 2) radio de cobertura de la misma, 3) Azimut (Enacom, 2018).
- 4) *Azimut*: el radio de cobertura de una antena puede ser dividido en tres líneas a las que denominan Azimut. Las Azimut cortan los sectores a la mitad. De este modo, conociendo la ubicación de cada Azimut respecto del Norte (grado 0) quedan definidos los tres sectores de la antena. Esto permitirá reducir la zona de interés del radio de cobertura en pos de establecer si el usuario de un teléfono

se encontró o no dentro de una zona de interés para la investigación (Enacom, 2019).

- 5) *Megadatos o datos GPRS*: es una tecnología de datos para redes de telefonía móvil que permite enviar y recibir paquetes de datos de manera eficiente, siendo que cada registro del mismo brindará el impacto en una celda y permitirá determinar las diferentes ubicaciones de un abonado a lo largo de un período de tiempo (Enacom, 2017).

Para finalizar el acápite, corresponde determinar en coincidencia con lo expuesto por Martínez (2020, p. 36), que la tercera fuente de recolección, la central de nuestro trabajo, es la información asociada brindada por las empresas prestatarias de servicios de telecomunicación (la primera sería a través de las escuchas telefónicas, y segunda con el secuestro del aparato celular a través del examen mediante software UFED¹).

Como veremos con más detalle, en breve se podrá solicitar información a las empresas prestatarias desde diferentes puntos de partida: 1) tráfico a partir de abonado, informando las prestatarias los registros de comunicaciones entrantes y salientes correspondientes; 2) tráfico a partir de celda, determinando una zona de interés y la prestataria devuelve los registros de comunicaciones entrantes y salientes de aquellas antenas, como también el impacto de megadatos o GPRS en dichas antenas; 3) tráfico de IMEI, cuándo se le brinda la numeración unívoca de un dispositivo a la prestataria y ésta aporta cuáles abonados (tarjetas SIM) impactaron en el dispositivo en cuestión.

3. La importancia de la utilización de un método

Como hemos venido desarrollando, la evidencia digital y en particular el análisis de las comunicaciones posee un bagaje técnico que complejiza su entendimiento. Por ello, el desarrollo de un método resulta fundamental no solo para no incurrir en errores a la hora de analizar los datos que aportan las compañías prestatarias de los servicios de comunicación, sino también para su publicidad y comprensión por la sociedad en su conjunto.

La dogmática penal ha desarrollado y estudiado por cientos de años un sistema o método lógico para establecer si una conducta específica constituye delito, esto es, una serie de niveles de análisis (acción típica, antijurídica y culpable) por los cuales el caso debe transitar para llegar a la conclusión de que existe delito (Hilgendorf y Valerius, 2017, p. 49; Rafecas, 2021, 177-185; Tarrío, 2015, 139-149). Este mismo sistema puede replicarse al tema aquí traído a análisis, a través del diseño de una serie de pasos que permita a cualquier interviniente o analista sacar diferentes conclusiones investigativas, pero a su vez que, al responder al mismo método investigativo, el proceso de acceso a las inferencias será conocido y comprendido por todos.

¹ UFED (Universal Forensic Extraction Device) es una herramienta desarrollada por la empresa Cellebrite, utilizada para la extracción, decodificación, análisis y presentación de datos digitales provenientes de dispositivos móviles. Esta tecnología permite recuperar información de teléfonos celulares y tarjetas SIM, incluso en casos donde los datos han sido eliminados o el acceso está restringido por bloqueos de seguridad. Información extraída de <https://cellebrite.com>.

En tal sentido, conforme la Real Academia Española, un método es un modo de decir o hacer con orden, pudiéndose referir también a un modo de obrar o proceder. Lo que aquí se propicia es un modo de hacer ordenado, mediante pasos lógicos que permitan sacar y evaluar conclusiones. Sentado ello, proponemos el estudio y aplicación de un método de examen de las comunicaciones de forma manual, claro y sencillo que pueda ser desarrollado por cualquier operador o analista con instrucción en la materia y entendido al ser explicado por estos por el resto de las personas.

Este método consiste en su inicio de cuatro simples pasos. Se parte solapadamente de una investigación en la cual las medidas de investigación convencionales en las primeras fases de la pesquisa han fallado, presuponiendo que en el hecho criminal investigado existe la sustracción de un teléfono celular. Ello no obedece a una cuestión de animosidad o ceguera, sino que pone al analista ante un panorama más complejo; el resto no ha funcionado y la sola investigación del equipo sustraído puede brindar diversas soluciones a la difícil situación en la que se encuentra el detective. Ahora bien, veremos también que, si se cuenta con información de los posibles involucrados en los hechos y sus posibles números de telefonía celular, el método podrá comenzar en un paso más avanzado resultando innecesario el inicio a través de los primeros pasos. Así también, en caso de no haber un equipo sustraído la investigación podrá comenzar en pasos subsiguientes con la información obtenida de otros métodos pesquisantes.

Como segunda advertencia, debemos decir que el camino de este método contará en todos sus pasos con una triple vertiente de ejecución, solicitud de información, recepción y análisis de dicha información, informe de lo analizado. Producido el triple canal de estudio, se continuará al siguiente paso de la misma forma: solicitud, análisis, informe.

Por último, en general en los procesos acusatorios mixtos y tal como se ha explicado *supra*, consideramos que la solicitud estará en cabeza del Ministerio Público Fiscal y podrá hacerlo directamente ante las empresas prestatarias, mediante oficio o portal de información, o bien, estableciendo como canal de diálogo entre el organismo judicial y las empresas a la DAJUDECO². Ejemplificaremos, como hemos advertido, a través del inicio de una investigación penal preparatoria en donde supondremos además que en el hecho delictivo se apoderaron ilegítimamente de al menos un teléfono celular.

Paso número 1:

Punto 1: Como primera medida, se solicitará a las empresas prestatarias de servicios de telefonía que informen, en base al número de línea del teléfono sustraído (obtención mediante testigos o sistemas de información), el listado de llamadas entrantes y salientes del abonado desde quince días antes de hecho hasta el día de la solicitud.

Como en cualquier otra medida de investigación, dicho paso posee una lógica de indagación criminal, que no es ni más ni menos que obtener el nro. de IMEI del equipo sustraído. Por ello, si se cuenta con ese dato previamente a través de la caja del teléfono celular o mediante alguna situación análoga, dicho punto del paso 1 no será necesario a menos que

² Dirección de Asistencia Judicial en Delitos Complejos y Crimen Organizado dependiente de la Corte Suprema de Justicia de la Nación, única dependencia estatal autorizada para realizar escuchas telefónicas legales y además funciona como enlace entre las autoridades judiciales y las empresas prestatarias a través de la sección información asociada de dicha dependencia.

se quiera contar previamente con un patrón de frecuencia comunicacional de la víctima en pos de establecer un posible móvil del hecho criminal investigado.

Punto 2: A su vez, se solicitará se informe el impacto y activación de megadatos o informe GPRS de dicho abonado, desde el día anterior al hecho hasta el día posterior. En este caso, el motivo de la solicitud tiene como objetivo investigativo evaluar el posible recorrido del teléfono sustraído luego del hecho –y por tanto de los incusos– si es que no lo apagaron a posterior del despojo, y de esta manera establecer el posible camino de huida de los imputados.

La solicitud abarca el día anterior al hecho, para establecer un patrón de frecuencia de antenas, es decir qué antenas son las habituales del usuario del teléfono sustraído para su posterior comparación; y del día posterior a fin de poder conocer si el aparato tuvo un período de “enfriamiento” para ser puesto en funcionamiento en las horas siguiente y determinar en qué lugar.

Paso número 2:

Luego de haber solicitado, analizado y realizado un informe a partir de la información descripta en el paso 1, se continuará con el paso nro. 2. Antes de emitir una nueva solicitud, se debe comprobar si el nro. de IMEI se corresponde con el equipo sustraído, para lo cual podemos recurrir a algunas páginas públicas³ con el objeto de constatar si el IMEI emergente del análisis de las comunicaciones se corresponde con el modelo informado por la víctima o sus familiares.

Verificada tal situación, en el paso nro. 2 se solicitará a todas las empresas de telefonía celular que informen si nuevos abonados telefónicos han impactado con posterioridad al ilícito investigado en el equipo sustraído (IMEI). Es importante aclarar que la solicitud no sólo será ante la empresa que brindaba servicio telefónico a la víctima, sino a todas las compañías. Ello en función a que el teléfono se puede encontrar “liberado”, es decir apto para su utilización en cualquier empresa de telefonía o puede ser “liberado” con posterioridad al hecho. El objetivo de este paso es determinar si, con posterioridad al hecho, el celular sustraído fue puesto en uso al colocarle un nuevo chip y, por tanto, encontrarse funcionando con otro nro. de abonado. Uno podría preguntarse cuál fue la utilidad del paso 1, punto 2. El recorrido del abonado de la víctima puede permitir orientar otras medidas investigativas, como por ejemplo el relevamiento de cámaras. Será de utilidad, además, en los pasos subsiguientes para el cotejo de celdas con los teléfonos de presuntos imputados.

Paso número 3:

De aquí en adelante, la solicitud será idéntica a la del paso nro. 1 pero mutando la variable de análisis. En este caso, la variable en estudio no será el abonado telefónico de la víctima sino aquel que haya emergido en una *check list* positiva de empresas prestatarias del paso nro. 2. Es decir, aquel abonado que haya sido inserto en el teléfono celular sustraído a la víctima.

³ Por ejemplo: <https://imeicheck.com/es/verificador-imei>.

Si la lista de control del paso nro. 2 ha arrojado resultado negativo en cuanto a nuevos impactos, en esta faceta de investigación de las comunicaciones se produce un corte en el camino y deberá trabajarse con otras variables comunicacionales, como ser impactos coincidentes en registros de antenas de interés, tema este que excede el objeto de este artículo. Asimismo, se puede recurrir a otras fuentes de pesquisa para poder partir con el teléfono de un imputado identificado desde este mismo punto. En este último caso, o bien si el paso nro. 2 ha arrojado resultado positivo, se deberá proceder de la siguiente manera:

Punto 1: Utilizando como variable el teléfono del presunto imputado o aquel que impactara en el IMEI que se corresponde con el equipo sustraído, se solicitarán llamadas entrantes y salientes desde 15 días antes del hecho hasta el momento de la solicitud. Ello tiene como objetivo crear un patrón de frecuencia comunicacional del imputado que, a la postre, será de utilidad en el paso nro. 4. Además, se deberán prestar especial atención a las llamadas que realice el usuario el día del hecho, así como el día anterior y posterior.

Punto 2: Quizás este sea el punto más importante del método explicado. Se solicitará del teléfono del sindicado o de aquel que impactara en el celular sustraído, informe de GPRS desde el día anterior al hecho hasta el día posterior. Lo que se busca, principalmente, con este pedido de información y análisis, es determinar la ubicación del teléfono celular del sindicado en el momento en que se estaba cometiendo el hecho investigado, pero también su movimiento antes y después del evento. Se deberá tener en cuenta, entre otras cuestiones, si con posterioridad al hecho su impacto de antenas resulta coincidente con el del abonado de la víctima extraído del paso 1 punto 2.

Es cierto que la geolocalización por este medio no dirá con exactitud la ubicación del usuario. Y, para mayor precisión, deberán estudiarse cuasi escalonadamente la ubicación de la antena, radio de cobertura, Azimut, tiempo de arribo de la señal⁴ y sectorización⁵. Sin perjuicio de ello, el estudio de este punto indicará un fuerte indicio de reprochabilidad en determinadas circunstancias. Tal es así que, si la persona imputada reside a unos cuantos kilómetros de distancia del lugar del hecho, pero gracias a los datos GPRS es posible ubicar el trayecto del teléfono desde cercanías de su domicilio hasta el lugar de comisión del injusto y luego volver a proyectar su recorrido hacia su lugar de residencia, esto importará un indicio probatorio de suma relevancia, todo lo que podrá ser plasmado en un mapa interactivo (por ejemplo, mediante la aplicación de Google Maps) que a la postre servirá didácticamente en la explicación ante la judicatura.

Debemos tener en cuenta que cada notificación, cada interacción que tenga el usuario del teléfono por medio de alguna aplicación como ser una red social (WhatsApp, Instagram, Facebook, etcétera) genera un impacto de datos GPRS, el cual se registrará en una antena cercana a la ubicación física del aparato.

Es gracias a ello que podemos trazar, luego de analizar la información, el recorrido de ese teléfono celular, e incluso podemos ubicarlo con mayor precisión si las compañías nos

⁴ La estimación del tiempo de llegada TOA por sus siglas en inglés (Time of Arrival) es una técnica de posicionamiento que permite medir la distancia, estableciendo así la ubicación. En este caso y sin perjuicio de que excede el eje del presente se tendrá en cuenta los factores tiempo distancia entre la ubicación de la celda y el teléfono celular.

⁵ La sectorización de la DAJUDECO permite visualizar en un mapa interactivo la zona aproximada de cobertura de cada celda utilizada por el abonado objeto de investigación. Visto en: www.mpfchubut.gov.ar/images/pdf/Resoluciones/2022/RES091-E_Anexo_DAJuDeCO.pdf.

proporcionan los datos requeridos de radio de cobertura y Azimut. Con ello, se adquirirá precisión en referencia al rango, forma y dirección de apertura, sin perjuicio de lo cual existen otros estudios para precisar más la cuestión.

Por último, si de este paso se obtuvieron resultados positivos, tanto sea que mediante llamadas o impactos de GPRS, habremos podido ubicar el teléfono que venimos analizando en cercanías al lugar del hecho al momento de su comisión, y por lo tanto arribar a algunas conclusiones parciales. Veamos.

El usuario de ese abonado, con la probabilidad que requiere la instancia, participó del hecho investigado. Ahora bien, es importante acreditar que el titular de dicho abonado es el usuario del teléfono. Así, para dar con su verdadera identidad es recomendable agregar el número a la aplicación WhatsApp para poder obtener su fotografía y *nickname* de aplicación y ver si coinciden con la titularidad o bien extraer su fotografía y mandar a cotejar al sistema de individualización criminal de Policía Federal. Otra herramienta útil es la simulación de una transferencia a través de la aplicación de Mercado Pago. En la Provincia de Buenos Aires también contamos con la aplicación cuenta DNI, que resulta ser similar a Mercado Pago, por lo que también se puede en ese caso realizar una simulación, considerando que ambos sistemas poseen requisitos de ingreso biométricos que hacen presumir que el usuario de la aplicación es el portador del abonado. Estas son algunas de las opciones, las más básicas y comunes en este tipo de investigaciones. Pero cada investigación posee diferentes desafíos, por lo que cada una de ellas nos va a llevar a adoptar distintas acciones.

Paso número 4:

Punto 1: Tal como hemos adelantado, desde el paso nro. 3 en adelante siempre se vuelve a realizar la misma solicitud de información, pero cambiando la variable de análisis. En el caso de este punto, se solicitarán llamadas entrantes y salientes desde 15 días antes del hecho de todos los abonados obtenidos en el punto 1 del paso 3 (patrón de frecuencia comunicacional del abonado obtenido en el paso nro. 2 o del presunto abonado de un imputado). Es decir, en el paso nro. 3 punto 1 se obtienen aquellos abonados con los cuales se comunica frecuentemente el teléfono de interés. Se pueden elegir los cinco, diez, quince o más teléfonos frecuentes, dependiendo de la gravedad de la investigación. Esto tiene como objetivo investigativo formar un patrón de frecuencia comunicacional de cada número en pesquisa ahora.

Punto 2: Respecto de todos los números obtenidos en el paso nro. 3 punto 1, se analizará su impacto de GPRS a fin de determinar si pueden ser ubicados en el lugar de los hechos o si presentan coincidencia de impactos con el abonado de la víctima, o bien con el del abonado que impactara en el celular sustraído o con el abonado identificado de un investigado. También permitirá acreditar si los usuarios de los abonados ahora en estudio pueden o no tener relación con el hecho investigado. Respecto a aquellos abonados de los cuales se obtenga un resultado positivo, deberá volverse al punto anterior (paso 4 punto 1), ver su frecuencia comunicacional y obtener aquellos abonados de utilidad para comenzar con la solicitud del paso nro. 5, y así sucesivamente dependiendo la cantidad de involucrados en el evento criminal.

4. Conclusión

A lo largo del presente hemos brindado una aproximación acerca de la importancia del avance de las nuevas tecnologías no solo en la vida cotidiana sino también en referencia a su injerencia en el Derecho Penal y por sobre todo en la investigación criminal. Entendemos que la comprensión del análisis de las comunicaciones resulta fundamental para propiciar investigaciones de calidad y poder así brindar un correcto servicio de justicia. En tal sentido, dimos a conocer que la formulación de un método de análisis permite no solo dotar de previsibilidad y seguridad a sus conclusiones sino también de entendimiento para los propios analistas, los operadores judiciales y la sociedad en su conjunto.

Como resultado de ello, hemos sentado que el método explica el caso, permite emitir conclusiones, formular y descartar hipótesis, pero que también el caso explica el método, desde la situación de hecho traída a conocimiento se logra una mejor comprensión de esta serie de pasos lógicos, que vaya paradoja fue creada para explicar los casos.

Poseemos la firme convicción de que este es solo un inicio, una forma de comunicar nuestra manera de entender el análisis de las comunicaciones, que puede ser robustecida, criticada, mejorada, alterada o bien sustituida por ideas superadoras, y que todo ello contribuirá en seguir avanzando hacia un sistema, lógico y complejo, pero previsible y entendible, de investigación criminal en base al examen de las comunicaciones. Dicho sea de paso, consideramos que no hay margen de dudas de que su explicación resulta ser la mejor manera para que tanto los operadores judiciales como la sociedad puedan entender de qué se trata.

Referencias

- ENACOM (2011). *Plan Fundamental de Numeración Nacional*, “Anexo III – Definiciones”, Buenos Aires.
- ENACOM (2016). Resolución 2459/2016, “Procedimiento para el bloqueo de terminales con reporte de robo, hurto o extravío y la identificación de IMEI irregulares”.
- ENACOM (2017). *Manual de conceptos básicos de telecomunicaciones y servicios móviles*, Buenos Aires.
- ENACOM (2018). “Radiobases para Servicios de Comunicaciones Móviles”.
- ENACOM (2019). “Parámetros técnicos para antenas de radiobases”.
- Fernández, Diego (2023). “Análisis doctrinal y Jurisprudencial”, Tomo I, en: Torres, Sergio G. y Basílico, Ricardo A. (directores), 2023. *Código Procesal Penal de la Provincia de Buenos Aires*. Hammurabi, Buenos Aires.
- Hilgendorf, Eric, Valerius, Brian (2017). *Derecho Penal*. “Parte General”. AD-HOC, Buenos Aires.
- Lorenzo, Leticia (2014). *Manual de Litigación*, Ediciones Didot, Buenos Aires.
- Martínez, Alejandro M. (2020). “Análisis de redes, comunicaciones telefónicas e investigación penal”, Repositorio institucional digital de acceso abierto de la Universidad de Quilmes, Buenos Aires.
- Ministerio de Seguridad de la Nación (2023) “Protocolo para la identificación, recolección, preservación, procesamiento y presentación de evidencia digital”. Visto en: <https://www.fiscales.gob.ar/wp-content/uploads/2023/04/MINSEG-MPFN-Protocolo-evidencia-digital-2.pdf>
- Ministerio Público Fiscal de la Ciudad autónoma de Buenos Aires (2013). “Protocolo de gestión de almacenamiento de la evidencia digital”, disponible en: <https://documentosboletinoficial.buenosaires.gob.ar/publico/PJ-RES-MPF-FG-107-23-ANX.pdf>

Rafecas, Daniel (2021). *Derecho penal sobre bases constitucionales*. Ediciones Didot, Buenos Aires.

Tarrío, Mario C., Tarrío, Gonzalo A. (2015). *Manual de Derecho Penal*. “Parte General”, Cathedra Jurídica, Buenos Aires.


CIBERSEGURIDAD Y GOBERNANZA GLOBAL: ENTRE BUDAPEST Y LA PROPUESTA DE NACIONES UNIDAS

Cybersecurity and Global Governance: Between Budapest and the United Nations Proposal

Rosa Merlin Rodríguez*

Universidad Nacional Autónoma de México

rmerlin@politicas.unam.mx

 <https://orcid.org/0009-0001-0191-4060>

RECIBIDO 14/11/2025 - ACEPTADO 17/11/2025

Resumen

El artículo compara el Convenio de Ciberdelincuencia del Consejo de Europa con la propuesta de Convención de la ONU. El Convenio ofrece procedimientos penales armonizados y cooperación ágil, pero su alcance regional y enfoque tecnocrático limitan su legitimidad y amplían tendencias punitivas. La Convención de la ONU aspira a legitimidad universal y mayor centralidad de los derechos humanos, aunque enfrenta obstáculos políticos y operativos. El trabajo propone un modelo de gobernanza híbrida que combine interoperabilidad técnica, sólidas salvaguardas de derechos y mecanismos multilaterales inclusivos para reducir desigualdades y fortalecer la ciberseguridad como herramienta de cooperación y justicia.

Palabras clave:

ciberspace, ciberseguridad, convenciones, gobernanza, ciberdelincuencia.

Abstract

The article compares the Council of Europe's Cybercrime Convention with the United Nations' proposal. The Convention offers harmonized criminal procedures and swift operational cooperation, but its regional scope and technocratic orientation limit its legitimacy and reinforce punitive approaches. The UN proposal seeks universal legitimacy and a stronger human rights focus, yet faces significant political and operational challenges. The article advocates for a hybrid governance model that combines technical interoperability, robust human rights safe-guards, and inclusive multilevel mechanisms to reduce inequalities and strengthen cybersecurity as a tool for cooperation and justice.

Keywords:

cyberspace, cybersecurity, conventions, governance, cybercrime.

1. Introducción

La seguridad hemisférica contemporánea se ha configurado bajo una lógica marcadamente multidimensional. Fenómenos como la transnacionalidad del crimen organizado, el terrorismo, el desarrollo acelerado de las tecnologías digitales y la expansión de internet no solo han redefinido la agenda internacional, sino que han colocado a la ciberseguridad como uno de los componentes estructurales del orden global. Esta transformación vuelve indis-

* Lic. en Derecho (Universidad Nacional Autónoma de México), Doctora en Derecho y Gobernanza Global (Universidad de Salamanca). Académica de la Facultad de Ciencias Políticas y Sociales de la UNAM.

pensable su estudio desde las Relaciones Internacionales, disciplina para la cual el ciberespacio constituye hoy un ámbito crítico de disputa de poder, regulación y legitimidad.

En América Latina, la construcción del sistema interamericano durante la Guerra Fría, articulada en torno al Tratado Interamericano de Asistencia Recíproca (TIAR) y la Organización de los Estados Americanos (OEA en adelante) y el liderazgo hegemónico de Estados Unidos configuró una noción de seguridad centrada inicialmente en amenazas estatales convencionales. No obstante, desde la fundación de la Junta Interamericana de Defensa (JID de ahora en adelante) en 1942 hasta la Declaración de Bridgetown de 2002, dicha noción ha evolucionado de forma sustancial. El punto de inflexión se produjo durante la Conferencia Especial de Seguridad celebrada en México en 2003, donde los Estados miembros de la OEA ampliaron el concepto de seguridad hacia un enfoque multidimensional, incorporando amenazas no tradicionales como: el terrorismo, la delincuencia transnacional y, de manera creciente, los ataques a la seguridad cibernética.

En este marco, la OEA a través del Comité Interamericano contra el Terrorismo (CICTE de ahora en adelante) ha incentivado la cooperación entre gobiernos, sector privado y sociedad civil para identificar vulnerabilidades y diseñar políticas nacionales en materia de ciberseguridad (Ibarra y Nieves, 2016). Estas acciones responden a una realidad contundente: las amenazas que emergen en el ciberespacio han reconfigurado drásticamente los paradigmas clásicos de seguridad internacional. A diferencia de los conflictos armados localizables territorialmente, las ciberamenazas se caracterizan por su deslocalización, su naturaleza multifacética y su rápida mutación.

Esta complejidad erosiona categorías jurídicas tradicionales como agresión, soberanía y responsabilidad internacional, que se ven tensionadas por la dificultad para atribuir ataques y por la presencia simultánea de actores estatales y no estatales operando desde múltiples jurisdicciones (Robles, 2016). El espectro de amenazas incluye desde delitos informáticos comunes como el fraude, robo de datos, explotación sexual infantil en línea hasta actividades más sofisticadas como el ciberespionaje estatal, el sabotaje digital y las acciones contra infraestructuras críticas. La distinción clásica entre cibercrimen, ciberterrorismo y ciber guerra se vuelve así insuficiente para dar cuenta de fenómenos que pueden superponer tácticas, actores y motivaciones en un mismo evento.

Los reportes recientes confirman esta tendencia. El “Global Threat Report 2024” de CrowdStrike registra un incremento del 60% en intrusiones interactivas durante 2023 y un aumento del 73 % en el segundo semestre, con el sector tecnológico como principal objetivo. Este patrón se intensificó durante la pandemia, cuando la digitalización masiva aumentó la superficie de ataque global. De manera paralela, el Fondo Monetario Internacional (2024) alerta sobre el riesgo de que los ciberataques funcionen como detonadores de crisis macrofinancieras, especialmente en sectores altamente digitalizados como el financiero.

Sin embargo, la problemática no es nueva. Desde el uso fraudulento del telégrafo en el siglo XIX hasta los *phreakers* de la década de 1970 que manipulaban sistemas telefónicos mediante *blue boxes*, la historia revela que la innovación tecnológica ha sido sistemáticamente acompañada de nuevas formas de criminalidad (Sain, 2018). La “Operación Diablo del Sol” de 1990, aunque con limitados efectos legales, constituye uno de los primeros precedentes de cooperación internacional contra la delincuencia informática (OGDI,

2016). La liberalización del comercio global en los años noventa propició aún más la expansión del cibercrimen transfronterizo, particularmente en el ámbito financiero (Sain, 2015).

Las Tecnologías de la Información y la Comunicación (TIC en adelante) han transformado la naturaleza de los delitos al ofrecer anonimato, bajo costo, alcance global y facilidad técnica. Esta evolución, señala Bartolomé (2020), reduce la barrera de entrada para los atacantes, diluye las fronteras jurídicas, dificulta la detección de incidentes y vuelve ineficaces los modelos clásicos de análisis del crimen. Zunzunegui agrega que la deslocalización y la existencia de jurisdicciones permisivas configuran “paraísos cibernéticos”, donde la persecución penal resulta prácticamente inviable (2008, p. 171).

Este panorama evidencia la necesidad urgente de contar con marcos normativos de alcance global que sean capaces de responder a la escala, la velocidad y la sofisticación de las amenazas contemporáneas en el ciberespacio. En este contexto, resulta particularmente relevante la comparación entre dos modelos internacionales de respuesta: el Convenio sobre la Ciberdelincuencia del Consejo de Europa (Convenio de Budapest de ahora en adelante), y la Convención de las Naciones Unidas contra la Ciberdelincuencia. Ambos instrumentos encarnan concepciones divergentes de gobernanza digital y revelan tensiones geopolíticas, conceptuales y de derechos humanos que atraviesan el debate actual sobre la regulación del entorno digital.

El Convenio de Budapest, vigente desde 2004, constituye el marco jurídico internacional más consolidado en la materia. Su aportación principal radica en la armonización de tipos penales, el establecimiento de procedimientos claros para la preservación y obtención de datos, la creación de mecanismos ágiles de cooperación operativa y el desarrollo de herramientas técnicas con más de dos décadas de aplicación acumulada. Estas características le otorgan estabilidad jurídica y una valiosa experiencia institucional. Sin embargo, su naturaleza regional y su fuerte orientación tecnocrática, así como su origen asociado a estándares impulsados predominantemente por Estados occidentales, han suscitado recelo entre diversos países del Sur Global. Para muchos de ellos, el Convenio continúa siendo insuficientemente universal y excesivamente inclinado hacia paradigmas punitivos y de vigilancia, lo que ha limitado su aceptación y ha reforzado críticas sobre su sesgo geopolítico.

En contraste, la propuesta de Convención de la Organización de las Naciones Unidas (ONU en adelante) se presenta como un esfuerzo por construir un marco verdaderamente universal, sustentado en un enfoque más amplio que incorpora la protección robusta de derechos humanos, principios de gobernanza inclusiva, el reconocimiento expreso de la soberanía digital y la articulación de mecanismos de cooperación multinivel. Aun así, este proyecto enfrenta desafíos significativos. Entre los más relevantes se encuentran las profundas divergencias políticas entre los distintos bloques de Estados, el riesgo de generar instrumentos sobrerregulatorios o susceptibles de politización, las dificultades técnicas inherentes a la armonización de estándares globales y la preocupación de que algunos gobiernos utilicen la ampliación de tipos penales como herramienta para restringir derechos fundamentales, reprimir la disidencia o limitar libertades en el espacio digital.

2. Formas de amenazas en el ciberespacio

La consolidación del ciberespacio como un dominio autónomo de interacción social, económica y política ha catalizado el surgimiento de nuevas formas de conflictividad que transgreden las categorías tradicionales del Derecho Internacional y desbordan los marcos normativos diseñados para regir escenarios físicos. En este sentido, la Estrategia Nacional de Ciberseguridad de España (2019) identifica tres manifestaciones paradigmáticas que configuran los principales focos de riesgo estructural en el entorno digital contemporáneo: el ciberdelito, el ciberterrorismo y la ciberguerra (Gutiérrez, 2020, p. 17). Estos fenómenos no sólo constituyen desafíos a la soberanía y la seguridad estatal, sino que también exigen un replanteamiento profundo de las herramientas jurídicas, institucionales y doctrinales aplicables a los conflictos digitales.

El ciberdelito, en su expresión más extendida, se refiere a conductas delictivas que se cometen mediante el uso de sistemas informáticos o contra estos, con una finalidad predominantemente lucrativa. Entre sus múltiples formas destacan las extorsiones realizadas a través de *ransomware*, el acceso no autorizado a bases de datos, la suplantación de identidad con fines de fraude (*phishing*), la distribución de malware para el robo o la manipulación de información, así como los ataques de denegación de servicio distribuido (DDoS, por sus siglas en inglés), que comprometen la operatividad de infraestructuras esenciales. Si bien la lógica económica es dominante, el ciberdelito no excluye móviles ideológicos o geoestratégicos, lo que evidencia una difuminación creciente de sus límites con otras expresiones de amenaza digital.

Por su parte, el ciberterrorismo representa una forma de violencia cuyo objetivo no es el beneficio material, sino la producción de efectos simbólicos o políticos, mediante el uso sistemático de las tecnologías digitales para generar miedo, subvertir el orden público o desestabilizar estructuras institucionales. En esta categoría se incluyen tanto el sabotaje informático contra servicios esenciales como redes eléctricas, sistemas de salud o transporte, como la propagación de contenidos extremistas, el reclutamiento virtual de simpatizantes o la planificación de actos de violencia mediante plataformas cifradas. Su carácter disruptivo no reside sólo en el daño técnico causado, sino en su capacidad para erosionar la confianza social y debilitar los pilares normativos del Estado constitucional.

La ciberguerra, finalmente, constituye la manifestación más sofisticada y potencialmente destructiva de la conflictividad interestatal en el ciberespacio. A diferencia del ciberterrorismo o el delito digital, aquí predomina la racionalidad estratégica de los Estados, que emplean capacidades ofensivas y defensivas cibernéticas como herramientas de proyección de poder, interferencia política o coerción indirecta. Estas operaciones –que pueden desplegarse de manera encubierta o abierta, autónoma o combinada con medios cinéticos– buscan alterar el equilibrio de poder internacional mediante la neutralización de infraestructuras críticas, la manipulación de procesos electorales o la interrupción de servicios soberanos. Conforme al Manual de Tallin sobre el Derecho Internacional aplicable a la Ciberguerra, este tipo de agresiones puede alcanzar la categoría de “uso de la fuerza” o “ataque armado” si sus efectos materiales son equiparables a los previstos en el artículo 51 de la Carta de las Naciones Unidas.

Estas tres formas no deben entenderse como compartimentos estancos, sino como tipos analíticos que comparten tecnologías, actores, plataformas y tácticas. La intersección de motivaciones políticas, económicas y militares da lugar a escenarios híbridos que desafían la capacidad del Derecho Internacional para clasificar, atribuir y sancionar adecuadamente estas conductas. En este contexto, la elaboración de una arquitectura jurídica coherente y eficaz exige superar las lógicas binarias propias del derecho penal clásico o del *ius ad bellum*, adoptando enfoques multidimensionales que integren elementos del Derecho Internacional humanitario, del Derecho Penal Internacional, de la protección de los derechos humanos y del régimen de cooperación interestatal.

El debate doctrinal ha intentado dar respuesta a este desafío mediante la proliferación de términos como ciberdelito, criminalidad informática o delincuencia digital, sin que hasta el momento se haya alcanzado una definición jurídica consolidada a nivel global. Esta dispersión terminológica no es meramente semántica: refleja la ausencia de consensos sobre los elementos normativos, sustantivos y procesales que deben estructurar el régimen internacional de combate a las amenazas digitales. Esta ambigüedad conceptual obstaculiza la armonización de legislaciones nacionales, debilita los marcos de cooperación judicial transfronteriza y favorece la impunidad, especialmente en contextos donde los Estados se muestran renuentes a tipificar estos actos o carecen de voluntad política para sancionarlos eficazmente.

En consecuencia, resulta indispensable avanzar hacia una sistematización jurídica del ciberconflicto, que articule marcos normativos robustos con mecanismos institucionales de coordinación y rendición de cuentas. Frente a una conflictividad que evoluciona con velocidad tecnológica y que erosiona silenciosamente la estabilidad del orden jurídico internacional, el Derecho está llamado no solo a reaccionar, sino a anticipar y regular con visión transformadora, en defensa de la paz, la legalidad y los derechos fundamentales en el entorno digital global.

Hasta ahora, la mayor parte de la legislación internacional sobre ciberdelitos ha priorizado la criminalización como principal respuesta: tipificar nuevas conductas delictivas o adaptar las ya existentes para enfrentar los retos del ciberespacio. Sin embargo, este enfoque resulta limitado. El Convenio de Budapest (2001) fue pionero al intentar ofrecer un marco más integral, que no solo incluyera delitos sustantivos, sino también normas procesales y mecanismos de cooperación internacional. Sus categorías abarcan ataques contra la confidencialidad, integridad y disponibilidad de datos, fraudes informáticos, delitos de contenido (como la pornografía infantil) e infracciones a derechos de autor.

A pesar de su resiliencia capaz de adaptarse a nuevas modalidades delictivas como las *botnets*, el instrumento deja vacíos importantes: el robo de identidad, el *grooming* a menores, el *spam* y el ciberterrorismo no fueron contemplados. Estas omisiones responden tanto a dificultades técnicas como a divergencias socioculturales. Por ejemplo, mientras que algunos países en desarrollo buscan penalizar el spam, las economías avanzadas lo tratan como un problema civil o administrativo. De este modo, el Convenio refleja un consenso mínimo más que un marco global comprehensivo. Además, su origen europeo y la falta de adhesión de potencias clave han limitado su legitimidad y alcance universal.

3. Perspectivas conceptuales de la ciberseguridad

El concepto de ciberseguridad, aunque relativamente reciente, abarca prácticas de seguridad informática que han evolucionado con el tiempo. Sin embargo, su definición es aún motivo de debate entre los Estados. Lo que antes se consideraba un asunto técnico limitado a la gestión de riesgos en infraestructuras críticas, hoy se ha convertido en una prioridad estratégica para la seguridad nacional. A medida que la digitalización avanza y transforma la economía, la sociedad y la política, las preocupaciones en torno a la ciberseguridad continúan creciendo, consolidando su papel central en la gobernanza global del ciberespacio.

Esta se ha consolidado como un eje central en la agenda política global, trascendiendo su impacto inicial en el ámbito estatal y empresarial para convertirse en un elemento clave de la geopolítica contemporánea. Como señalan Dunn Cavelty y Wenger (2019), su alcance se ha expandido hacia una multiplicidad de esferas políticas, reflejando su creciente complejidad y la interconexión con cuestiones estratégicas más amplias. Este fenómeno evidencia que la ciberseguridad ya no puede abordarse únicamente desde una perspectiva técnica, sino que requiere un enfoque integral que considere sus implicaciones en la seguridad nacional, la economía digital y la gobernanza global del ciberespacio.

Según Josep Ibañez (2011), surge como una respuesta indispensable para contrarrestar las amenazas originadas en el ciberespacio, un ámbito donde interactúan actores diversos en un entramado complejo. Esta dinámica demanda un enfoque de gobernanza que logre equilibrar los distintos intereses involucrados, tales como la protección de datos, la seguridad nacional y las libertades individuales.

En este contexto, la seguridad cibernética se convierte en un campo de disputa y cooperación entre diferentes actores, reflejando las dinámicas de poder y las asimetrías globales. Maximiliano Vila y Marcelo Saguier (2019) destacan que la digitalización reconfigura las relaciones de poder, dando paso a nuevas formas de hegemonía digital, donde los actores dominantes se benefician de un control creciente sobre el ciberespacio.

Ésta es entendida como el esfuerzo por salvaguardar la integridad de los sistemas digitales, la confidencialidad de la información y la disponibilidad de infraestructuras. La ciberseguridad se ha consolidado como una cuestión crítica tanto en el ámbito privado como público, tal como proponen Singer y Friedman (2014). En el sector empresarial, resulta esencial para mantener la eficiencia y rentabilidad sin comprometer la seguridad de empleados y clientes. A nivel estatal, sin embargo, ha adquirido un carácter prioritario, convirtiéndose en una cuestión de seguridad nacional.

Vargas y Recalde (2017) subrayan que la creciente sofisticación de los ciberataques ha obligado a los gobiernos a invertir en capacidades de ciberdefensa y a formular políticas para disuadir o responder ante estas amenazas. Este fenómeno refleja un cambio significativo hacia la ciberseguridad como una estrategia clave del Estado. En muchos casos, este enfoque se ve reforzado por una perspectiva securitizadora, donde se aborda desde una óptica militar y de defensa. Vila y Saguier (2019) critican esta hegemonía de la perspectiva estratégica, señalando cómo ha desplazado la visión libertaria original de los pioneros de internet.

El proceso de securitización de la ciberseguridad, sin embargo, no está exento de controversias. Según Vila y Saguier (2019), las nuevas formas de poder y las asimetrías generadas

en el ámbito digital revelan un orden hegemónico configurado por actores predominantes, ya sean Estados o corporaciones tecnológicas. Estos actores, al ocupar una posición central en la gobernanza digital, ejercen una influencia significativa sobre las normas y políticas que rigen el ciberespacio. No obstante, los autores también señalan que los países de América Latina, y en general aquellos que experimentan nuevas formas de dependencia tecnológica, enfrentan grandes dificultades para participar activamente en la configuración de este orden mundial digital, lo que evidencia una brecha en la gobernanza global que debe ser abordada.

Los enfoques de Ibáñez (2011), Singer y Friedman (2014), Vargas y Recalde (2017), y Vila y Saguier (2019) nos presentan un escenario complejo en el que las dinámicas de poder, las vulnerabilidades cibernéticas y las estrategias de seguridad nacional convergen. Este entorno globalizado e interdependiente evidencia las crecientes tensiones entre la protección de la privacidad, la soberanía digital y la seguridad colectiva. Las políticas y estrategias de ciberseguridad deben reconocer estas asimetrías y tensiones, adoptando un enfoque inclusivo que contemple no solo los intereses de los actores más poderosos, sino también los de aquellos que se ven más afectados por las dinámicas de la digitalización y la ciberseguridad global.

En la literatura de la política internacional, la ciberseguridad se presenta como un campo de creciente tensión geopolítica, donde potencias como China, Estados Unidos y Rusia desempeñan papeles clave en la formulación de sus estrategias de seguridad cibernética. Chang (2014) señala que la ciberseguridad ha dado lugar a comunidades especializadas en el pensamiento estratégico, donde China y Estados Unidos adoptan enfoques diferenciados. A medida que el ciberespacio se convierte en un nuevo terreno de disputa global, las relaciones de poder, hegemonía y soberanía digital se hacen cada vez más evidentes.

En el caso de China, la narrativa de la ciberseguridad se caracteriza por la ambición de convertirse en una potencia cibernética global, como afirma Shen (2016). Bajo el liderazgo de Xi Jinping, la ciberseguridad ha sido posicionada como un objetivo estratégico prioritario, con el propósito no solo de proteger su infraestructura, sino también de dominar el ciberespacio. Esta postura contrasta con la de Estados Unidos, que, según Ülgen (2016), enfrenta constantes ciberataques debido a su posición como superpotencia. En este contexto, Estados Unidos se ha visto obligado a desarrollar una estrategia nacional de protección de infraestructura cibernética, consolidando un enfoque de “resolución de problemas” que busca mantener el orden hegemónico neoliberal. Este modelo se refleja también en las políticas de gobernanza de internet, donde Estados Unidos promueve un modelo de múltiples partes interesadas, que busca equilibrar el poder entre actores estatales y no estatales, pero que también refleja su dominio sobre las normas internacionales.

Rosa Piñón (2018) critica que, en términos de ciberseguridad, la gobernanza global sigue siendo una tarea pendiente debido a la falta de consenso y las divergencias entre actores internacionales. La pluralidad de estrategias, junto con una regulación jurídica obsoleta, complica la creación de un marco de cooperación que permita una gobernanza efectiva en el ciberespacio. Según Piñón, la ciberseguridad no puede entenderse solo como una respuesta a las amenazas, sino como un campo donde tanto Estados como actores no estatales utilizan el ciberpoder para posicionarse y proteger sus intereses, lo que genera tensiones sobre las normas de gobernanza global.

El análisis de Ülgen (2016) también subraya la complejidad de la ciberseguridad como un ámbito de acción estatal y defensa, donde Rusia, con su legado soviético, se ha convertido en un actor clave en la ejecución de ciberataques, reflejando la rivalidad tecnológica entre las grandes potencias. En este contexto, el poder cibernético no solo está relacionado con la protección de sistemas, sino también con la afirmación de poder y soberanía en un mundo digital cada vez más interconectado.

Las perspectivas conceptuales de la ciberseguridad, como lo subrayan los distintos autores, indican que este tema no es solo una cuestión técnica, sino también una arena de conflicto geopolítico, donde las potencias emplean el ciberpoder como una extensión de su influencia y control sobre el orden mundial. Por lo que la gobernanza de la ciberseguridad debe analizarse no solo en términos de amenazas y soluciones, sino también en relación con las dinámicas de poder que subyacen a la construcción de las normas y estrategias de seguridad global.

La ciberseguridad es un campo en constante evolución que trasciende los enfoques tradicionales de análisis y demanda una perspectiva interdisciplinaria. Su impacto en la sociedad se intensificará a medida que las nuevas tecnologías digitales amplíen los límites del ciberespacio y den lugar a problemáticas aún más complejas. La interacción entre la ciberseguridad, los cambios socioeconómicos y el desarrollo del Estado plantea un desafío crucial: garantizar que las soluciones tecnológicas no solo respondan a amenazas emergentes, sino que también contribuyan a una gobernanza digital equilibrada y sostenible (Dunn Cavelty y Wenger, 2019).

El estudio de la ciberseguridad exige una perspectiva profundamente interdisciplinaria, capaz de responder a la velocidad de los cambios tecnológicos y a las transformaciones del entorno político global. Desde el ámbito jurídico, resulta indispensable comprender la ciberseguridad como un asunto de interés para el derecho y la justicia, debido a su impacto directo en la prevención de delitos y en la mitigación de afectaciones que trascienden la infraestructura crítica del Estado. Estas problemáticas incluyen la protección de datos personales, el robo de identidad, el fraude digital y otras conductas que pueden vulnerar derechos humanos fundamentales.

En este contexto, se vuelve necesario adoptar un enfoque que combine la cooperación internacional con formas de colaboración amplia entre los distintos actores que participan, inciden o resultan afectados en este ecosistema. Solo a través de esta articulación será posible construir respuestas más integrales y efectivas frente a las amenazas del ciberespacio.

4. El Convenio sobre la Ciberdelincuencia en el marco del Consejo de Europa

El Convenio sobre Ciberdelincuencia, también conocido como “Convenio de Budapest”, es un tratado promovido por el Consejo de Europa en 2001 para mejorar la cooperación entre países y crear marcos legales coherentes contra la ciberdelincuencia y la actividad delictiva en internet.

En cuanto a su estructura, éste consta de 48 artículos y un preámbulo. En concreto encontramos cuatro capítulos, divididos en secciones y títulos. El primer capítulo tan sólo comprende un precepto, referido a la terminología usada en el texto. El capítulo segundo,

“Medidas que deberán adoptarse a nivel nacional”, incluye elementos tanto de Derecho material (responsabilidad penal, tentativa, complicidad, etc.) como procesal (procedimiento, salvaguardas, datos, registros, jurisdicción, etc.). En cuanto al tercero, se introduce directamente en la cooperación internacional. Abarca cuestiones como la extradición, la asistencia entre Estados, la información, el intercambio de datos y el establecimiento de una red 24/7. El último capítulo contiene las disposiciones finales propias de un Tratado internacional: adhesión, entrada en vigor, aplicación territorial, efectos, régimen de reservas, denuncias, notificaciones, etc.

Ha sido ratificado por 31 Estados de Europa y los Estados Unidos de América con el propósito de combatir la cibercriminalidad y promover la cooperación transnacional en este ámbito. Argentina, Chile, Costa Rica, Colombia, Panamá, Paraguay, Perú y República Dominicana son los países latinoamericanos que han suscrito el Convenio, mientras que Brasil, Ecuador, Guatemala, México son observadores.

El Convenio de Budapest es ampliamente reconocido como un punto de referencia en los esfuerzos globales para fortalecer el Estado de Derecho en el ciberespacio. No solo fue el primer tratado internacional en este campo, sino que también sigue siendo uno de los instrumentos jurídicos más importantes como un modelo para naciones interesadas en elaborar leyes integrales contra los delitos cibernéticos y como un marco para la colaboración internacional entre los países que son parte de este tratado.

Entre sus aspectos clave se encuentran la tipificación como delito de acciones como el acceso no autorizado, los ataques a la integridad de sistemas y datos, el fraude informático y los delitos vinculados a la pornografía infantil. Además, ofrece herramientas legales que mejoran la efectividad de las investigaciones sobre ciberdelitos y la obtención de pruebas electrónicas, al tiempo que fomenta una cooperación internacional rápida y eficiente en este ámbito.

Sin embargo, no define específicamente el término ciberdelito o cibercrimen, sino que se centra en las conductas criminales relacionadas con la informática que los Estados parte deben incluir en sus leyes internas. En el Artículo 1 establece una serie de definiciones tales como sistema informático, datos informáticos, proveedor de servicios y datos relativos al tráfico.

Los Títulos 1, 2, 3, 4 de dicho convenio establece una serie de delitos a saber:

Cuadro 1
Delitos contenidos en el Convenio sobre la Ciberdelincuencia

Clasificación	Tipo de delitos
Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos	Acceso ilícito Interceptación ilícita Ataques a la integridad de datos Ataques a la integridad del sistema
Delitos informáticos	Falsificación informática Fraude informático

Delitos relacionados con el contenido	Delitos relacionados con la pornografía infantil Abusos a los dispositivos
Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines	Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines

Fuente: Elaboración propia a partir del Convenio sobre la Ciberdelincuencia. Apoyo con ChatGPT.

Como se puede observar en el Cuadro 1, estas conductas se dividen en delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos; delitos informáticos como falsificación y fraude; delitos relacionados con contenido como pornografía infantil; y delitos de propiedad intelectual y derechos afines. Además de las disposiciones penales, el convenio también abarca aspectos procesales, jurisdiccionales y un sistema detallado de cooperación internacional para combatir este tipo de crimen.

Respecto a las medidas que han de adoptarse a nivel nacional, el Convenio establece que cada país firmante debe implementar medidas legislativas y otras acciones necesarias para tipificar como delitos, en su jurisdicción nacional, los siguientes actos (Consejo de Europa, 2001):

- 1) Acceso deliberado e ilegítimo a todo o parte de un sistema informático (Art. 2).
- 2) Interpretación deliberada o legítima por medios técnicos, de datos informáticos transmitidos en comunicaciones no públicas en un sistema informático (Art. 3).
- 3) Ataques a la integridad de datos como todo acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos (Art. 4).
- 4) Obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático (Art. 5).
- 5) Comisión deliberada e ilegítima de la producción, venta, obtención para uso, importación, difusión u otra forma de disponibilidad de dispositivos en programas informáticos y contraseñas, con el propósito de cometer los delitos mencionados anteriormente (Art. 6).
- 6) Falsificación informática, fraude informático, pornografía infantil, delitos relacionados con infracciones a la propiedad intelectual y derechos similares (Arts. 7, 8, 9 y 10).

El Convenio de Budapest también establece la penalización de delitos como la tentativa y la complicidad, así como la responsabilidad legal de las entidades jurídicas. Además, indica que las sanciones deben ser efectivas, proporcionadas y disuasorias, incluyendo penas privativas de libertad. Cada Parte del Convenio conserva la jurisdicción para juzgar delitos cometidos en su territorio, en buques o aeronaves bajo su bandera, por sus nacionales en ciertas circunstancias, o cuando ningún Estado tiene competencia territorial.

En este sentido establece un marco legal para la cooperación internacional en delitos que implican pruebas electrónicas. Va más allá de la ciberdelincuencia. Facilita la firma del Segundo Protocolo Adicional al Convenio de Budapest, mejorando la cooperación y la divulgación de pruebas electrónicas y permitiendo la colaboración directa con proveedores

de servicios en diferentes países y en situaciones de emergencia. También permite a los Estados Parte formar parte del Comité del Convenio sobre la Ciberdelincuencia para intercambiar información, evaluar la aplicación del Convenio y ofrecer orientación interpretativa. Esto fomenta la cooperación entre el sector privado y las autoridades de justicia penal. Además, los países que se adhieran pueden recibir asistencia técnica para mejorar su capacidad de cooperación internacional y aplicar plenamente el Convenio.

Por lo que la cooperación internacional en la lucha contra el delito informático requiere una visión global y conjunta, ejecutando políticas integradoras mediante una gobernanza global. Es crucial involucrar a todos los Estados y sectores de la sociedad en políticas conjuntas, priorizando convenios multilaterales sobre tratados bilaterales para armonizar las políticas regionales en cibercrímenes y lograr una regulación coherente a escala global, a pesar de los desafíos existentes en el entendimiento entre países y el entramado legislativo.

5. La Convención de las Naciones Unidas contra la Ciberdelincuencia (UNCC)

La Convención de las Naciones Unidas contra la Ciberdelincuencia (UNCC, por sus siglas en inglés y de ahora en adelante), aprobada mediante la Resolución A/RES/79/243¹, representa un hito normativo en el sistema multilateral al establecer un marco jurídico integral y universal para abordar el uso delictivo de las tecnologías de la información y la comunicación. A diferencia del Convenio de Budapest de 2001, que ha sido criticado por su enfoque eurocentrista y por haber sido negociado sin participación plena de muchos países en desarrollo, esta nueva Convención surge de un proceso intergubernamental abierto, inclusivo y universal, iniciado por la resolución 74/247 (2019) y continuado con la 75/282 (2021)², lo que le otorga una mayor legitimidad democrática en el seno de la ONU. Las cuales sentaron las bases para la elaboración de un instrumento jurídicamente vinculante capaz de responder a las amenazas que emergen del ciberespacio.

A través de la Resolución 74/247, se creó un comité intergubernamental especial con el mandato de elaborar una convención internacional sobre el uso delictivo de las tecnologías de la información y las comunicaciones (Asamblea General de las Naciones Unidas, 2024) tomando como base los esfuerzos nacionales, regionales e internacionales ya existentes.

En 2021, la Resolución 75/282 consolidó el mandato del Comité Especial, estableciendo su sede operativa entre Nueva York y Viena, con el objetivo de presentar un texto definitivo ante la Asamblea en su 78° período de sesiones (Asamblea General de las Naciones Unidas, 2024). Este proceso estuvo guiado por la necesidad de una cooperación internacional más robusta, especialmente ante la creciente sofisticación de los delitos cibernéticos y sus impactos negativos en el desarrollo sostenible, la seguridad global y el estado de derecho.

La resolución 79/243 reconoce explícitamente los desafíos contemporáneos derivados del uso indebido de las TIC y la disparidad en las capacidades estatales para hacerles frente (Asamblea General de las Naciones Unidas, 2024). Se manifiesta una clara intención de armonizar normas sustantivas y procesales en materia penal internacional, al tiempo que

¹ Resolución A/RES/79/243, adoptada el 24 de diciembre de 2024 por la Asamblea General de la ONU, disponible en: <https://docs.un.org/es/A/RES/79/243>

² Disponibles en: <https://docs.un.org/es/A/Res/74/247> y <https://docs.un.org/es/A/RES/75/282>, respectivamente.

se fomenta el respeto a los derechos humanos, la soberanía estatal y la diversidad jurídica de los sistemas nacionales.

Con un proceso de negociación que se extendió por más de un lustro y que involucró no solo a los Estados Miembro, sino también a actores no estatales incluyendo organizaciones de la sociedad civil, el sector académico y empresas tecnológicas, el texto final refleja un delicado equilibrio entre intereses divergentes.

La Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC, por sus siglas en inglés) asumió el rol de secretaría técnica durante las negociaciones, reforzando su papel central como órgano coordinador en la lucha global contra el crimen organizado (Asamblea General de las Naciones Unidas, 2024).

La Convención contra la Ciberdelincuencia ha sido abierta a firma en 2025, en Hanói, Vietnam, y entrará en vigor una vez que cuarenta Estados la ratifiquen (Asamblea General de las Naciones Unidas, 2024). Sin duda, esta convención representa un esfuerzo multilateral para enfrentar el uso indebido de las tecnologías de la información y la comunicación, cuya utilización delictiva se ha intensificado en escala, rapidez y alcance, superando las capacidades de respuesta tradicionales.

En el preámbulo y disposiciones iniciales, se reitera la urgencia de fortalecer la cooperación internacional frente a una amenaza cada vez más compleja y transfronteriza como lo es la ciberdelincuencia, destacando sus implicaciones negativas para la economía, el Estado de derecho y el desarrollo sostenible.

El Capítulo I, titulado Disposiciones Generales, introduce una aproximación renovada al tratamiento jurídico de los delitos cometidos mediante tecnologías digitales.

En dicho instrumento se proponen tres objetivos centrales establecidos en el art. 1 (Asamblea General de las Naciones Unidas, 2024):

- 1) Reforzar las medidas de prevención y combate a la ciberdelincuencia;
- 2) Fortalecer la cooperación internacional para hacer frente a este fenómeno;
- 3) Fomentar la asistencia técnica y el desarrollo de capacidades, con especial énfasis en el apoyo a los países en desarrollo.

A diferencia de la Convención de Budapest, que se enfoca predominantemente en delitos contra sistemas informáticos, la nueva Convención de las Naciones Unidas adopta un enfoque más amplio y transversal, al contemplar la utilización de las TIC en la comisión de delitos graves como el blanqueo de capitales, la corrupción, el terrorismo, la trata de personas, el tráfico ilícito de migrantes, armas, drogas y bienes culturales (Asamblea General de las Naciones Unidas, 2024). También destaca por incorporar con claridad la transmisión de pruebas electrónicas como un componente esencial de la cooperación penal internacional.

Los Capítulos III y IV de esta Convención representan un avance normativo significativo en la lucha contra la ciberdelincuencia, al establecer con mayor precisión y amplitud los criterios de jurisdicción y las medidas procesales que los Estados deben implementar para investigar y sancionar eficazmente estos delitos (Asamblea General de las Naciones Unidas, 2024). Reconociendo la complejidad propia del entorno digital, la normativa busca

equilibrar la necesidad de cooperación internacional y flexibilidad jurisdiccional con la protección de los derechos humanos.

Observamos que en el Capítulo III, dedicado a la jurisdicción, se amplían los supuestos que permiten a un Estado ejercer su competencia penal. Más allá del tradicional criterio territorial, la Convención contempla que la jurisdicción pueda extenderse a casos donde el delito afecte a nacionales, residentes o al propio Estado, incluso si la conducta se origina fuera de su territorio con la intención de causar un daño dentro de él (Asamblea General de las Naciones Unidas, 2024). Además, se promueve la coordinación entre Estados ante investigaciones simultáneas, lo cual contribuye a evitar duplicidades y conflictos, fortaleciendo la cooperación internacional.

Esta perspectiva supone una evolución frente al Convenio de Budapest de 2001, que adoptaba un enfoque más restrictivo, centrado en la jurisdicción territorial y la nacionalidad del autor, sin considerar expresamente escenarios transnacionales tan complejos ni mecanismos coordinados tan desarrollados. La nueva Convención responde así a las transformaciones tecnológicas y a la naturaleza global y descentralizada del cibercrimen, donde las fronteras tradicionales pierden eficacia para delimitar la acción delictiva.

Por su parte, el Capítulo IV aborda las medidas procesales y herramientas legales necesarias para la persecución penal en el ámbito digital. Se incorporan procedimientos detallados para la conservación acelerada de datos electrónicos, la emisión de órdenes para obtener información almacenada, la búsqueda e incautación de evidencia digital y la recolección en tiempo real tanto de datos de tráfico como de contenido de comunicaciones. Además, se destacan salvaguardas dirigidas a proteger los derechos fundamentales, como la proporcionalidad, la supervisión judicial y la confidencialidad, junto con medidas específicas para la protección de testigos y víctimas, lo que refleja un enfoque integral y respetuoso de los derechos humanos (Asamblea General de las Naciones Unidas, 2024).

En comparación con el Convenio de Budapest, que sentó las bases para la cooperación en ciberdelincuencia, pero ofrecía disposiciones menos detalladas en estas materias, esta Convención aporta una actualización y profundización importante. Destaca, además, el reforzamiento de los mecanismos para el embargo, incautación y decomiso de productos del delito, incluyendo la facultad para acceder a documentación bancaria y financiera, adaptándose mejor a la sofisticación de los delitos económicos y tecnológicos contemporáneos.

Lo cual evidencia un esfuerzo renovado por adecuar el marco jurídico internacional a las exigencias del ciberespacio actual, enfatizando una jurisdicción más flexible y una robusta capacidad procesal, sin perder de vista la protección de derechos fundamentales, lo que representa una respuesta más efectiva y contemporánea que el modelo planteado en Budapest en 2001.

Esta Convención se proyecta como un instrumento multilateral de segunda generación, con mayor alcance temático, legitimidad política e implicaciones normativas, especialmente para los países del Sur Global que hasta ahora habían tenido una participación limitada en los marcos existentes. Sin embargo, su efectividad dependerá de su implementación nacional, de los mecanismos de cooperación técnica que se establezcan y de su articulación con los principios del Derecho Internacional de los Derechos Humanos. De este

modo, se sientan las bases para una arquitectura jurídica internacional más robusta, adaptada a los desafíos complejos de la era digital.

Al posicionarse como instrumento global, este instrumento jurídico aspira a cerrar las brechas normativas, prevenir refugios seguros para ciberdelincuentes y garantizar un equilibrio entre eficacia penal y respeto a las garantías fundamentales en la era digital. No obstante, su implementación práctica enfrentará retos significativos. La eficacia del instrumento dependerá de la voluntad política de los Estados parte para armonizar sus marcos legales internos, asignar recursos suficientes y participar activamente en los mecanismos de cooperación internacional que establece. Sin esta articulación, las disposiciones del tratado corren el riesgo de quedarse en el plano declarativo.

La Convención de las Naciones Unidas contra la Ciberdelincuencia, adoptada en 2024, surge como un intento de establecer el primer instrumento multilateral de carácter verdaderamente global. A diferencia de Budapest, la UNCC fue negociada en el marco de la Asamblea General de la ONU, lo que le otorga mayor legitimidad política y cobertura potencial. Retoma elementos de convenios previos como Budapest y la Convención Árabe de 2010, pero introduce innovaciones relevantes:

- 1) *Jurisdicción ampliada*: incorpora el principio de personalidad pasiva, permitiendo a un Estado ejercer competencia cuando sus nacionales resulten afectados, incluso si el delito ocurrió en el extranjero.
- 2) *Mecanismos institucionales*: establece la Conferencia de los Estados Parte y una Secretaría permanente, algo que Budapest no contempla, para supervisar la implementación y coordinar con organismos como la UNODC.
- 3) *Salvaguardas jurídicas*: incluye cláusulas explícitas sobre proporcionalidad, revisión judicial independiente y prohibición de extradición en casos de persecución política, religiosa o de género, en un esfuerzo por balancear seguridad con derechos humanos.

No obstante, la UNCC también enfrenta críticas significativas. Algunos observadores advierten riesgos de vigilancia excesiva y censura, pues el tratado legitima la recolección de datos por parte de los Estados, aunque sujeta a controles legales. Asimismo, la cláusula de personalidad pasiva puede abrir la puerta a usos con motivaciones políticas, especialmente en países con instituciones débiles.

En términos comparativos, el Convenio de Budapest se caracteriza por su flexibilidad y por haber sentado las bases normativas regionales que inspiraron otros instrumentos. Sin embargo, su carácter eurocéntrico, las limitaciones temáticas y la ausencia de potencias tecnológicas restan eficacia a su alcance global. Por su parte, la UNCC representa un avance sustantivo hacia la universalización de un marco jurídico contra la ciberdelincuencia, con innovaciones procesales e institucionales que refuerzan la cooperación internacional. Aun así, su eficacia dependerá de la voluntad política de los Estados parte, de la aplicación efectiva de las salvaguardas y de su capacidad de evitar que se convierta en una herramienta de control estatal incompatible con la democracia y los derechos humanos.

En definitiva, ambas convenciones presentan fortalezas y limitaciones: Budapest, como referente técnico y precursor regional; la UNCC, como un esfuerzo multilateral más inclusivo y con vocación global. Su coexistencia marcará el futuro de la gobernanza global en

materia de ciberdelincuencia, donde la cooperación y la confianza mutua serán determinantes.

6. El caso de México

A más de dos décadas de la apertura a firma del Convenio de Budapest sobre la Ciberdelincuencia, México permanece como Estado observador, sin haber formalizado su adhesión. Esta omisión resulta particularmente significativa dada la creciente sofisticación y frecuencia de los delitos informáticos en el país, y evidencia un desfase normativo respecto de los estándares internacionales vigentes en la materia. A pesar de exhortos legislativos, como el emitido por el Senado en septiembre de 2021 (Ballinas y Becerril, 2021), el Poder Ejecutivo no ha formalizado la ratificación, lo que refleja una reticencia institucional que no puede entenderse como prudencia legislativa, sino como una manifestación de la debilidad estructural del sistema penal frente a los desafíos del entorno digital.

Desde una perspectiva jurídica, la resistencia mexicana se articula en torno a la tensión entre el derecho penal nacional y los compromisos que emanan del Derecho Internacional de los tratados. Conforme al Artículo 133 de la Constitución Política de los Estados Unidos Mexicanos (CPEUM, por sus siglas y de ahora en adelante) los tratados internacionales ratificados por México tienen jerarquía equiparable a las leyes federales, lo que implica su aplicabilidad directa una vez publicados. Sin embargo, el orden constitucional también impone límites materiales: los Artículos 1 y 133 prohíben celebrar tratados que alteren los derechos humanos reconocidos por la propia Constitución, mientras que los Artículos 14 y 16 establecen el principio de legalidad penal, en su vertiente del *nullum crimen, nulla poena sine lege*.

Estos últimos consagran el principio de legalidad penal, lo que implica que ninguna persona puede ser sancionada sin que exista previamente una norma jurídica que tipifique de forma clara y específica la conducta sancionable. De este modo, se prohíbe constitucionalmente la imposición de penas que no se encuentren expresamente previstas en una ley vigente y aplicable al caso concreto.

La Suprema Corte de Justicia de la Nación (SCJN, por sus siglas y de ahora en adelante) ha sostenido que la descripción legal de un delito no puede ser vaga, ambigua ni sujeta a interpretaciones extensivas, ya que ello vulneraría la seguridad jurídica y abriría espacio a la arbitrariedad judicial³. En este sentido, ha enfatizado que los tipos penales deben contener "un contenido concreto y unívoco", estableciendo con claridad el bien jurídico tutelado, los elementos del tipo y los rangos punitivos correspondientes.

El Convenio de Budapest exige a los Estados Parte dos obligaciones fundamentales: primero, tipificar como delitos ciertas conductas relacionadas con el uso de tecnologías de la información, como el acceso ilícito a sistemas informáticos, la interceptación de datos, la alteración de información digital, la obstrucción de servicios, el abuso de dispositivos, la falsificación y el fraude informático, entre otros; y segundo, conferir a las autoridades judiciales y ministeriales poderes adecuados para investigar y sancionar tales delitos, incluyen-

³ Ver: Tesis Jurisprudencial, 1a./J. 10/2006, Novena Época, Semanario Judicial de la Federación y su Gaceta. Tomo XXIII, marzo de 2006, p. 84.

do la vigilancia de comunicaciones, la recolección de datos de tránsito, el aseguramiento de evidencia digital y la colaboración transnacional.

En el caso mexicano, la incorporación de estas obligaciones no puede realizarse sin un proceso riguroso de armonización legislativa. Diversas disposiciones contenidas en el Convenio, particularmente los artículos 2 al 8, emplean conceptos como “ilegítimo” o “posesión” sin ofrecer una definición cerrada, lo que entra en fricción con el principio de legalidad penal en su dimensión de ley cierta y estricta. Por ejemplo, el artículo 2 sobre acceso ilícito y el artículo 6 sobre abuso de dispositivos, podrían interpretarse de manera tan amplia que habilitaran la persecución de conductas ambiguas, como el uso no autorizado de redes institucionales o la tenencia de herramientas informáticas utilizadas en pruebas de seguridad digital.

Además, la legislación penal mexicana no existe una sistematización suficiente en materia de ciberdelitos. El Código Penal Federal (CPF, por sus siglas y de ahora en adelante), si bien contempla algunas figuras delictivas relacionadas con la informática, lo hace de forma dispersa, sin un capítulo específico y sin tipificación integral. Esta fragmentación obstaculiza la aplicación homogénea de la ley y dificulta la capacitación de los operadores jurídicos. En este contexto, Danya Centeno (2018) ha propuesto la incorporación de un título específico sobre delitos informáticos en el CPF, lo que facilitaría la adecuación normativa al Convenio, garantizando claridad, coherencia y protección de derechos fundamentales.

Asimismo, debe considerarse la aplicación del principio de culpabilidad, que implica que la imposición de penas sólo puede realizarse sobre la base de hechos concretos imputables al sujeto, y no sobre su personalidad o supuesta peligrosidad. La ambigüedad de los tipos penales previstos en el Convenio podría derivar en un uso punitivo desproporcionado, especialmente en un contexto como el mexicano, donde se ha documentado el uso arbitrario de tecnologías de vigilancia por parte de autoridades estatales.

La no ratificación del Convenio de Budapest por parte de México no puede ser atribuida únicamente a una omisión política. Se trata de una decisión que evidencia tensiones estructurales entre el derecho penal nacional y los compromisos internacionales, y que requiere una estrategia legislativa articulada para asegurar que la adhesión al tratado no vulnere principios constitucionales ni habilite el uso discrecional del poder punitivo del Estado. Mientras no se subsanen las deficiencias normativas internas y se establezca un marco penal técnico y constitucionalmente compatible con los estándares del Convenio, su ratificación resultará no solo inviable, sino también riesgosa desde el punto de vista de los derechos fundamentales.

A más de dos décadas de su adopción, el Convenio Budapest permanece sin ratificación por parte de México, a pesar de los crecientes riesgos estructurales que enfrenta el país en el entorno del ciberespacio y de los múltiples llamados institucionales para revisar su estatus jurídico. En septiembre de 2021, el Senado mexicano exhortó al Poder Ejecutivo a concluir la evaluación de dicho instrumento, subrayando su importancia para articular una política criminal eficaz en el ciberespacio (Ballinas y Becerril, 2021). Sin embargo, la postura de México no necesariamente obedece a una postura estratégica deliberada, sino que más bien revela una tensión estructural persistente entre la necesidad de armonizar el marco jurídico nacional con los estándares internacionales y las restricciones constitucio-

nales que rigen el derecho penal interno. Esta ambivalencia ilustra los dilemas normativos que enfrenta el país ante la expansión de una criminalidad transnacional cuya naturaleza digital exige respuestas jurídicas igualmente transfronterizas.

Dicho Convenio establece que los Estados parte deben adoptar medidas legislativas, administrativas y de otra índole que les permitan tipificar penalmente, dentro de su jurisdicción, una serie de conductas relacionadas con los sistemas informáticos. Estas conductas abarcan:

- El acceso intencional y no autorizado, total o parcial, a un sistema informático (Artículo 2).
- La interceptación deliberada e ilegítima, mediante herramientas técnicas, de datos transmitidos en comunicaciones no públicas dentro de un sistema informático (Artículo 3).
- Las afectaciones a la integridad de los datos, como su alteración, supresión, deterioro o eliminación de forma deliberada y sin autorización (Artículo 4).
- La interferencia intencional y no autorizada que cause una interrupción significativa en el funcionamiento de un sistema informático (Artículo 5).
- La creación, adquisición, distribución o cualquier forma de facilitación de herramientas –incluyendo software, dispositivos o contraseñas– destinadas a la comisión de los delitos anteriores (Artículo 6).
- Otros delitos como la falsificación informática, el fraude informático, la pornografía infantil y las infracciones a los derechos de propiedad intelectual o derechos afines (Artículos 7 a 10).

Estas disposiciones reflejan no solo un esfuerzo por establecer un lenguaje penal común frente a las amenazas cibernéticas sino también un intento de fomentar la cooperación internacional y la asistencia jurídica mutua entre los Estados. Empero, la adhesión plena al Convenio implica también un ejercicio complejo de adecuación normativa que, en el caso mexicano, se enfrenta al reto de armonizar las disposiciones internacionales con el principio de legalidad penal, los límites al *ius puniendi* y la protección de los derechos fundamentales previstos en la Constitución.

Es decir, este rezago se torna más apremiante cuando se consideran los efectos jurídicos de la eventual ratificación. Conforme al artículo 133 de la CPEUM, los tratados internacionales válidamente celebrados por el Estado mexicano forman parte del derecho interno. Ello implicaría que, una vez ratificado, el Convenio de Budapest tendría eficacia directa y vinculante para jueces y autoridades nacionales. No obstante, esta aparente ventaja jurídica plantea complejidades de compatibilidad si se analiza a la luz del principio de legalidad penal consagrado en los artículos 14 y 16 constitucionales, que exige una definición precisa, clara y estricta de los tipos penales.

En este sentido, el Convenio de Budapest presenta ambigüedades sustanciales en la redacción de algunas de sus figuras típicas como el acceso ilícito, la interceptación ilegal o el uso indebido de dispositivos al utilizar expresiones genéricas como “sin derecho”, “de forma ilegítima” o “con fines delictivos” sin especificar el bien jurídico protegido o los límites objetivos de la conducta punible. Este tipo de formulaciones abiertas, si bien útiles para sistemas de derecho anglosajón o mixto, entra en tensión con la tradición penal garantista

del ordenamiento mexicano, que exige una taxatividad absoluta en la formulación normativa para evitar tanto la impunidad como la discrecionalidad punitiva (Centeno, 2018).

El debate, por tanto, no se limita a lo técnico, sino que implica una tensión estructural entre la apertura internacional del derecho penal y los límites de un constitucionalismo mexicano. Este vacío normativo contrasta con la realidad de vulnerabilidad digital que enfrenta el Estado mexicano. En los últimos años, el país ha sido blanco de ciberataques de alto impacto, incluyendo incidentes dirigidos contra infraestructuras críticas como PEMEX (la petrolera estatal), el IMSS (seguridad social), la Secretaría de Economía o la propia Secretaría de la Defensa Nacional. La sofisticación de los ataques que van desde campañas de *ransomware* hasta intrusiones persistentes avanzadas evidencia que la falta de adhesión al Convenio de Budapest no es una simple omisión diplomática, sino una renuncia táctica a construir un marco normativo de respuesta articulada frente a amenazas transnacionales.

La adhesión de México requerirá una reingeniería normativa orientada a garantizar compatibilidad entre el tratado y los principios rectores del derecho penal nacional. En términos legislativos, dos rutas se perfilan como posibles: la creación de una ley especial en materia de delitos informáticos, o bien la modificación sustancial del Código Penal Federal para incorporar los tipos penales previstos en el Convenio. Si bien la primera opción puede ofrecer ventajas pedagógicas y especialización técnica, su implementación efectiva sería limitada en un sistema caracterizado por la falta de articulación normativa, escasa capacitación judicial y reducida interoperabilidad institucional. Por el contrario, una reforma integral al CPF permitiría una inserción orgánica del Convenio en el marco penal vigente, evitando duplicidades normativas y asegurando coherencia entre los principios sustantivos y las reglas de imputación penal (Centeno, 2018).

La ciberseguridad enfrenta importantes retos estructurales, derivados de la ausencia de un marco legal integral y de la fragmentación regulatoria entre múltiples agencias. Aunque instituciones como la Fiscalía General de la República, la CNBV, el Banco de México, el INAI y la Guardia Nacional desempeñan funciones específicas en la protección del ciberespacio, la falta de coordinación y estandarización de políticas limita la eficacia de las acciones preventivas y reactivas frente a incidentes cibernéticos. Este panorama resalta la necesidad de fortalecer la gobernanza institucional, promover la cooperación interinstitucional y desarrollar un marco normativo integral, que permita a México enfrentar de manera más sólida las amenazas cibernéticas y garantizar la protección de la infraestructura crítica y los derechos digitales de la ciudadanía (Vela-Treviño y Villanueva-Plasencia, 2025).

En el ámbito internacional, ha reafirmado su compromiso con la cooperación y actualización del marco normativo para enfrentar delitos cibernéticos, proteger datos personales y garantizar derechos humanos (Salas, 2025), a través de la celebración de la Convención de las Naciones Unidas contra la Ciberdelincuencia en diciembre de 2024 en Hanoi, Vietnam, aunque aún no la ha ratificado. Este acto refuerza dicho compromiso, mientras que las cifras del Reporte Global de Amenazas 2025, que registran 35,200 millones de intentos de ciberataques en los primeros tres meses del año, posicionan a México como el segundo país más afectado de la región y evidencian la urgencia de implementar políticas robustas de ciberseguridad (Salas, 2025).

De tal forma que el verdadero desafío no radica en firmar el tratado, sino en transformar el sistema jurídico interno para responder con legalidad, proporcionalidad y eficacia a las amenazas digitales del siglo XXI. Solo así podrá el Estado mexicano avanzar hacia una soberanía digital robusta, que conjugue seguridad, cooperación internacional y protección efectiva de los derechos humanos en el entorno digital.

7. Hacia una gobernanza híbrida para la ciberseguridad y la justicia digital

En correspondencia con lo anteriormente expuesto, ni Budapest ni la Convención de la ONU, por sí solos, pueden resolver la complejidad del ecosistema cibernético actual. Por ello, se propone avanzar hacia un modelo de gobernanza híbrida, que integre:

- interoperabilidad técnica entre instrumentos,
- salvaguardas estrictas de derechos humanos,
- cooperación operativa ágil y multilateral,
- mecanismos inclusivos que reduzcan asimetrías geopolíticas,
- fortalecimiento de capacidades en países con pocos recursos,
- participación activa del sector privado, la academia y la sociedad civil.

Este modelo permitiría armonizar el enfoque tecnonormativo del Consejo de Europa con la búsqueda de legitimidad global y justicia digital impulsada desde la ONU. La ciberseguridad, entendida no solo como protección técnica sino como condición para el ejercicio de derechos y la cohesión democrática, requiere de una arquitectura de gobernanza compleja, adaptativa y cooperativa.

Sin ello, el ciberespacio corre el riesgo de consolidarse como un ámbito de impunidad estructural, donde las brechas regulatorias erosionen los cimientos del derecho internacional contemporáneo.

8. Conclusiones

La comparación entre el Convenio de Budapest y la propuesta de Convención de la ONU revela que ambos instrumentos responden a lógicas normativas y políticas distintas, pero potencialmente complementarias. Mientras el primero privilegia la estandarización técnico-jurídica y la eficiencia operativa, el segundo busca articular un marco verdaderamente universal que incorpore principios de derechos humanos, soberanía digital y gobernanza inclusiva. Esta divergencia no solo refleja diferencias en capacidades estatales o prioridades nacionales, sino también las tensiones geopolíticas que estructuran el orden digital contemporáneo.

Si bien el Convenio de Budapest aporta una base probada y ampliamente implementada cuya eficacia práctica constituye una ventaja difícil de ignorar sus limitaciones respecto de legitimidad global, diversidad de modelos regulatorios y sensibilidad a desigualdades estructurales resultan cada vez más evidentes. Por otro lado, la Convención de la ONU, aun con su ambición normativa y su potencial democratizador, enfrenta riesgos de fragmentación política, estancamiento negociador y posibles usos indebidos por parte de regímenes autoritarios.

Ante este escenario, la solución no pasa por elegir entre uno u otro modelo, sino por avanzar hacia un esquema de gobernanza digital híbrido y pragmático. Tal enfoque implica:

- promover la interoperabilidad técnica sin sacrificar garantías de derechos,
- fortalecer mecanismos de cooperación multinivel que reduzcan las brechas de capacidad entre Estados;
- asegurar procesos de gobernanza más inclusivos, con participación significativa del Sur Global, de la sociedad civil y de actores técnicos;
- y consolidar salvaguardas que prevengan la instrumentalización política de la normativa penal.

México se encuentra en un momento decisivo: avanzar hacia un marco integral de ciberseguridad no solo implica establecer regulaciones y agencias, sino también consolidar una visión estratégica, multidimensional y prospectiva, que posicione al país con capacidad de respuesta frente a los desafíos del ciberespacio.

Referencias

- Ballinas, V., y Becerril, A. (2021, 15 de septiembre). Urgen a que México firme el Convenio de Budapest. *La Jornada*: <https://www.jornada.com.mx/notas/2021/09/15/politica/urgen-a-que-mexico-firme-el-convenio-de-budapest/>
- Bartolomé, M. (2020). *Ciberseguridad: retos y perspectivas en el ámbito global*. Instituto Español de Estudios Estratégicos: <https://www.ieee.es>
- Centeno, D. (2018). *México y el Convenio de Budapest: posibles incompatibilidades*. Red en Defensa de los Derechos Digitales / Derechos Digitales.
- Chang, A. (2014). “China’s cybersecurity strategy”. Center for a New American Security. Disponible en: <http://www.jstor.com/stable/resrep06327>
- Consejo de Europa. (2001). “Convenio sobre la Ciberdelincuencia” (Convenio de Budapest), disponible en: <https://www.coe.int>
- CrowdStrike. (2024). Global Threat Report 2024. CrowdStrike Inc.: <https://www.crowdstrike.com>
- Dunn Cavelty, M., y Wenger, A. (2019). *Cyber security politics: Socio-technological transformations and political fragmentation*. Routledge.
- Fondo Monetario Internacional. (2024). Informe sobre la estabilidad financiera mundial: abril de 2024, disponible en: <https://www.imf.org>
- Gutiérrez, E. (2020). “La responsabilidad internacional por el uso de la fuerza en el ciberespacio”. Aranzadi.
- Ibáñez, J. (2002), “Poder y autoridad en las relaciones internacionales: el control del comercio electrónico” [tesis de doctorado, Universitat Pompeu Fabra]. Tesis Doctorals en Xarxa. Disponible en: <https://www.tdx.cat/handle/10803/7281#page=1>
- Ibarra, J., y Nieves, J. (2016). “La seguridad cibernética en el sistema interamericano: avances y desafíos”. Organización de los Estados Americanos – CICTE.
- Naciones Unidas. (2022–2024). A/RES/74/247: Elaboración de una convención integral sobre la lucha contra el uso de las TIC con fines delictivos.

Oficina del FBI. (1990). “Operation Sun Devil”. U.S. Department of Justice.

OGDI. Observatorio de Delitos Informáticos. (2016). “Historia del cibercrimen y cooperación internacional”.

Organización de Estados Americanos. (2002). Declaración sobre Seguridad en las Américas (Declaración de Bridgetown). OEA.

Organización de Estados Americanos. (2003). Conferencia Especial sobre Seguridad: Declaración de México. OEA, disponible en: <https://www.oas.org>

Piñón, R. (2018). “La gobernanza global, la seguridad internacional y la Unión Europea amenazadas por un mundo convulso”. Centro de Estudios Latinoamericanos Facultad de Ciencias Políticas y Sociales UNAM: <https://doi.org/10.22201/cela.24484946e.2018.41.64146>

Robles, J. (2016). *Ciberseguridad y Derecho Internacional: soberanía, jurisdicción y atribución de responsabilidad*. Instituto Matías Romero.

Sain, M. (2015). *Cibercrimen y globalización económica: riesgos y desafíos*. Universidad de La Plata.

Sain, M. (2018). “Historia del delito informático: de los telégrafos al hacking moderno”. *Revista de Estudios sobre Seguridad*.

Salas, C. (2025, 27 agosto). “México y la ONU refuerzan alianzas para enfrentar ciberdelitos y fortalecer la ciberseguridad en Iberoamérica”. *Infobae*: <https://www.infobae.com/mexico/2025/08/27/mexico-y-la-onu-refuerzan-alianzas-para-enfrentar-ciberdelitos-y-fortalecer-la-ciberseguridad-en-iberoamerica/>

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.

Ülgen, S. (2016). “Cybersecurity” en: *Governing cyberspace: A Road Map for Transatlantic Leadership*. Carnegie Endowment for International Peace. <http://www.jstor.org/stable/resrep26924.11>

Vela-Treviño, C., y Villanueva-Plasencia, D. (2025, enero 7). *Cybersecurity in Mexico: A comprehensive overview*. Baker McKenzie Connect on Tech, en: <https://connectontech.bakermckenzie.com/cybersecurity-in-mexico-a-comprehensive-overview/>

Vila, M. y Saguier, M. (2019). “Ciberpolítica, digitalización y relaciones internacionales: un enfoque desde la literatura crítica de economía política internacional”. *Revista de Relaciones Internacionales*, n.º 40, 113–131: https://revistas.uam.es/relacionesinternacionales/article/download/relacionesinternacionales2019_40_005/10824/25587

Zunzunegui, S. (2008). “Delitos informáticos y jurisdicción internacional: retos del cibercrimen”. *Revista de Derecho y Tecnología*, 12, 165–184.