Reflexiones a 30 años del reconocimiento constitucional del habeas data. Hábeas data en la era digital: Límites y desafíos a 30 Años de su reconocimiento constitucional[*]

María Julia Giorgelli[**]

Resumen

El artículo analiza la evolución y los desafíos del hábeas data en Argentina, a tres décadas de su incorporación en la Constitución Nacional. Se hace foco en su nacimiento como una herramienta fundamental para garantizar la autodeterminación informativa y el derecho al honor y cómo ha sido cuestionada debido a la acelerada transformación tecnológica. Se examina la Ley 25.326 de Protección de Datos Personales, destacando su rol histórico junto a la necesidad imperante de una actualización que contemple nuevas realidades. Se analiza la adhesión de Argentina al Convenio 108 y su versión modernizada ("Convenio 108 plus") del Consejo de Europa como un marco legal que logra dar mejor protección a los derechos de las personas. Asimismo, se exponen algunas de las tensiones entre la privacidad y el avance tecnológico, ejemplificadas en casos que tomaron estado público.

Palabras clave: derechos humanos, vigilancia, privacidad, tecnología

Resumo

Este artigo analisa a evolução e os desafios do habeas data na Argentina, três décadas após sua incorporação à Constituição Nacional. Concentra-se em seu surgimento como ferramenta fundamental para garantir a autodeterminação informacional e o direito à honra, e como tem sido questionado devido à rápida transformação tecnológica. Examina a Lei 25.326 de Proteção de Dados Pessoais, destacando seu papel histórico e a necessidade urgente de uma atualização que aborde as novas realidades. Analisa a adesão

[*] Recibido: 14-03-2025. Aceptado: 08-07-2025

[**] Facultad de Derecho, Universidad de Buenos Aires; Escuela de Abogados del Estado; Argentina. Centro de Tecnología y Sociedad, Facultad de Derecho, Fundación Getulio Vargas, Brasil. Correo electrónico: giorgelli43@gmail.com

da Argentina à Convenção 108 do Conselho da Europa e sua versão modernizada ("Convenção 108 plus") como um arcabouço jurídico que protege melhor os direitos individuais. Apresenta também algumas das tensões entre privacidade e avanço tecnológico, exemplificadas em casos que se tornaram públicos.
Palavra chave: direitos humanos, vigilância, privacidade, tecnologia

Summary

This article analyzes the evolution and challenges of habeas data in Argentina, three decades after its incorporation into the National Constitution. It concentrates on its emergence as a fundamental tool to guarantee informational self-determination and direct honor, and as it has been questioned due to rapid technological transformation. Examines Law 25.326 of the Protection of Personal Data, highlighting its historical role and the urgent need for an update that addresses the new realities. Analyzes the Argentine adhesion to Convention 108 of the European Council and its modernized version ("Convention 108 plus") as a legal archive that best protects individual rights. It also presents some of the tensions between privacy and technological advance, exemplified in cases that become public.
Keywords: human rights, surveillance, privacy, technology

Introducción: marco conceptual del habeas data.

Hace 30 años, a pesar de no haber sido contemplado en la ley que fijó las bases de la reforma constitucional de 1994, el habeas data era incorporado al marco constitucional argentino en un valioso artículo 43. Su inclusión respondió a la necesidad de garantizar constitucionalmente la autodeterminación informativa, el derecho al honor y la privacidad. Es una herramienta centrada en las personas que permite exigir la supresión, rectificación, actualización o sometimiento a confidencialidad de la información personal.

En los años 1998 y 1999, el máximo tribunal de nuestro país admitió dos reclamos emblemáticos: Urteaga (CSJN Fallos: 321:2767) y Ganora (CSJN Fallos: 322: 2139). En el primero, un familiar de José Benito Urteaga -militante en los años setenta del Ejército Revolucionario del Pueblo (ERP)- pidió acceder a las circunstancias de la desaparición de su hermano, la Corte aceptó la pretensión y además reconoció su legitimación activa.

En el segundo, dos abogados defensores de un marino condenado por delitos de lesa humanidad, frente al supuesto de que estaban siendo escuchados, plantearon un reclamo judicial que también fue resuelto favorablemente.

Este nacimiento distintivo, ligado a los derechos fundamentales, le otorga al habeas data una jerarquía y potencia significativa. Por un lado, los fallos dan cuenta de la operatividad de los derechos constitucionales al afirmar, que pueden ser invocados y ejercitados a pesar de la falta de reglamentación legislativa, ello revela un impacto directo y real de la Constitución en la vida de las personas. Pero además, se advierte una relación con el proceso de restauración democrático iniciado en el año 1983 .

Tanto la reforma constitucional como las sentencias, fueron la consecuencia de un momento histórico y demandas que se materializaron post dictadura militar en la que la vigencia de los derechos personalísimos tuvieron un rol fundamental.

En definitiva, la evolución del marco legal y jurisprudencial en materia de derechos personalísimos en Argentina es un testimonio del compromiso del país con la defensa de los derechos humanos y la construcción de una sociedad más justa e igualitaria.

Aspectos normativos del habeas data.

En el año 2000, Argentina sancionó la Ley 25.326 de Protección de Datos Personales, alineándose con una tendencia global iniciada en la década de 1990. Esta legislación, centrada en la protección de la privacidad individual y no colectiva del derecho, establece principios fundamentales, herramientas y escenarios diversos relacionados con los datos personales. No obstante, en la actualidad, se trasluce la necesidad de una actualización que prevea los cambios tecnológicos y garantice este derecho en el entorno digital

La norma define a los datos personales como toda información relativa a un sujeto determinado o determinable. El concepto incluye un concepto en desuso. Se trata de la protección de las personas jurídicas que ya no es reconocida en las legislaciones más modernas. El objetivo, que sigue vigente hoy, consiste en garantizar el derecho al honor y la intimidad de las personas y establece una serie de herramientas para ese objetivo. Es también una figura versátil ya que puede dar solución a una variada gama de situaciones del Derecho como: rectificar antecedentes comerciales desfavorables, permitir el acceso a una historia clínica o bien solicitar comprender la lógica de funcionamiento sobre los datos de entrenamiento de una inteligencia artificial.

La Justicia de nuestro país analizó en varias ocasiones las tensiones entre el derecho a la privacidad y el interés en acceder a información pública. Un caso clave fue el impulsado por la ONG CIPPEC en el año 2014. El debate central giró en torno a si la divulgación de los padrones de beneficiarios de transferencias y subsidios sociales otorgados de los años 2006 y 2007 violaba la protección de datos personales sensibles. Finalmente, la Corte priorizó el derecho de acceso a la información pública[1].

En cuanto a la legislación argentina dedica una sección importante a los datos sensibles, definiéndose como aquellos que revelan información sobre el origen racial o étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical, o datos relativos a la salud o la vida sexual. Sin embargo, se observa una falta de actualización en esta definición, ya que no incluye explícitamente datos biométricos o genéticos, los cuales deben considerarse sensibles ante el avance de diversos avances tecnológicos actuales.

El precepto hace referencia a un concepto fundante del campo: la autodeterminación informativa. El mismo se define como la posibilidad que tiene cada individuo de controlar su información personal y saber que hacen los terceros que poseen los datos en calidad de depositarios. La figura es tomada del instituto acuñado por el Tribunal Constitucional Federal Alemán en el año 1983 con ocasión de verificar la inconstitucionalidad de la ley del censo de ese país[2].

Expertos en la materia sugieren que el marco conceptual del habeas data debe complementarse con las disposiciones del Código Civil relativas a los derechos personalísimos. Esto es, cuando se establece que cualquier persona cuya intimidad personal o familiar, honor, reputación, imagen o identidad sea vulnerada, o cuya dignidad personal sea menoscabada, tiene derecho a solicitar la prevención y reparación de los daños sufridos. Efectivamente las previsiones fortalecen y amplían las garantías ofrecidas por la ley de habeas data.

Los principios generales más importantes son el de calidad, licitud y finalidad. El primero garantiza que la información personal debe ser exacta, proporcional, razonable y la mínima necesaria para la tarea emprendida. También debe asegurarse la veracidad y

[1] Fallos “Cippec" -2014-, "Giustiniani" -2015-, "Garrido" -2016-, "Savoia" -2019

[2] Sentencia BVerfGE 65, 1 sobre censo de población, pág. 94. https://www.kas.de/c/document_library/get_file?uuid=0a66a4a6-1683-a992-ac69-28a29908d6aa&groupId=252038

que los datos personales no sean utilizados para una finalidad diferente o incompatible a la que motivó su obtención. Además el tratamiento de datos será lícito siempre que el titular hubiere prestado su consentimiento libre, expreso e informado, por un medio escrito o similar.

Se garantiza la gratuidad de los derechos de los titulares, los deberes de los responsables de los bancos de datos, las sanciones ante incumplimientos y también previsiones procesales aplicables a la sede judicial. Crea lineamientos sobre: seguridad de la información, transferencia de datos, tratamiento con fines de defensa nacional o seguridad pública por parte de las fuerzas armadas, fuerzas de seguridad e informes sobre servicios de información crediticia.

Sintetizando, se trata de una norma completa, garantista y útil en su tiempo que a la luz de las transformaciones sociales hoy obliga a su modernización.

Un paso significativo hacia la modernización de la protección de datos en Argentina fue la adhesión, en 2019, al Convenio 108 del Consejo de Europa relativo al tratamiento automatizado de datos personales. Posteriormente, nuestro país también aprobó el "Convenio 108 modernizado o plus", una versión actualizada de dicho tratado. Aunque este último aún no ha entrado en vigor, ya que requiere la ratificación de un mayor número de estados, su aprobación representa un avance crucial para el marco legislativo de argentina sobre protección de datos[3].

Asimismo, surgieron diversas propuestas para reformar la ley actual. Todas ellas siguen el modelo de la legislación europea, abrevando en las previsiones del Reglamento Europeo de Protección de Datos Personales (RGPD). El RGPD fue sancionado en el año 2016 y entró en vigor en el año 2018, es una norma comunitaria, robusta, que en once capítulos logra fortalecer los derechos fundamentales a la privacidad y los datos personales de los individuos en la era digital. Por su aplicación, han habido avances sustanciales como la creación de estándares sobre la reputación individual en el entorno on line y acciones de enforcement concretas mediante la aplicación de multas millonarias a grandes empresas tecnológicas con motivo del inadecuado tratamiento, recolección y utilización de los datos personales. El cuerpo constituyó una novedad al extender la jurisdicción y alcanzar así a las compañías extranjeras que tratan datos de residentes de la Unión Europea.

[3] Leyes 27.483 y 27.699.

En Argentina, el último proyecto de ley fue presentado en el año 2023 y dado que el mismo perdió estado parlamentario fue nuevamente presentado en el año 2025[4]. Durante el año 2022 el mismo contó con un interesante proceso participativo que, mediante el aporte de especialistas de diversos sectores, enriqueció la versión inicial desarrollada por el órgano garante. En agosto del año pasado fue debatido en comisión en la Cámara de Diputados de la Nación, aunque sin otros avances: por ende, de seguir esa situación a fin de este año perdería estado parlamentario. En su oportunidad, la autoridad administrativa señaló que el objetivo de la propuesta fue dar respuesta a los nuevos desafíos que imponen las transformaciones tecnológicas, el desarrollo de la economía digital y, a su vez, armonizar la legislación frente a los estándares regionales e internacionales, desde un enfoque de derechos humanos[5].

La modificación apuntó a ampliar el campo del habeas data y sobre todo abordar nuevas realidades con motivo del avance tecnológico. El principio de extraterritorialidad es un punto clave al igual que el Reglamento General de Protección de Datos Personales (RGPD) dado que otorga una competencia útil y acorde al mundo digital. También suma principios modernos como el de transparencia, minimización y responsabilidad proactiva y demostrada.

Se determinan nuevas bases legales que permiten el tratamiento de los datos personales generando de tal manera una transformación en el paradigma existente hasta el momento. En cuanto a los derechos de los titulares de los datos incorpora el de oposición y portabilidad. De igual manera reconoce medidas para la mejora de la protección de los datos personales como el aumento de multas, la figura del delegado de protección de datos, la evaluación de impacto y mejoras sobre la protección de datos personales para el caso de niñas, niños y adolescentes.

> En el plano mundial, a enero de este año el especialista David Banisar indica que
>
> 160 países y jurisdicciones y territorios autónomos de todo el mundo han adoptado leyes o reglamentos integrales de protección de datos/privacidad para proteger los datos personales en poder de entidades privadas. En general, alrededor del 82% de la población mundial vive en una jurisdicción con leyes o reglamentos de protección de datos (Banisar, 2024).

[4] https://www.argentina.gob.ar/sites/default/files/mensajeyproyecto_leypdp2023.pdf
[5] https://www.argentina.gob.ar/aaip/datospersonales/proyecto-ley-datos-personales

En el contexto regional, en marzo de este año, se notificó la primera sentencia de la Corte Interamericana de Derechos Humanos que reconoce el derecho a la autodeterminación informativa. El caso se denomina "Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" Vs. Colombia" (Serie C No. 506). Allí se señaló que "... Colombia vulneró, en perjuicio de las víctimas, los derechos a la vida, a la integridad personal, a la vida privada, a la libertad de pensamiento y de expresión, a la autodeterminación informativa, a conocer la verdad, a la honra, a las garantías judiciales, a la protección judicial, a la libertad de asociación, de circulación y de residencia, a la protección de la familia, los derechos de la niñez y el derecho a defender los derechos humanos". El tribunal realizó una interpretación contundente respecto a la Convención Americana sobre Derechos Humanos al afirmar que de la misma se permite derivar como un derecho autónomo a la autodeterminación informativa.

La decisión recoge acciones previas, como por ejemplo el trabajo del Comité Jurídico Interamericano de la Organización de Estados Americano (OEA). A comienzos del año 2012 se elaboraron una serie de estándares que fueron actualizados en el año 2021. Los mismos se conocen como los "Principios Actualizados sobre la Privacidad y la Protección de Datos Personales"[6] y si bien no conforman legislación positiva constituyen soft law y con ello una excelente guía para garantizar el derecho en América.

Documentos de este tipo son necesarios dado que delinean mejores prácticas nacionales e internacionales en planos cada vez más específicos a los que se enfrenta el Derecho. En tal sentido proponen estándares flexibles con el objetivo de que sean viables según los sistemas jurídicos y realidades de cada país.

Sin embargo, queda pendiente en la región, una legislación común que aborde la problemática. Reconociendo esa necesidad en Julio de 2024, se presentó una iniciativa que propone la discusión de una "Convención Interamericana sobre Tratamiento de Datos Personales, Autodeterminación Informativa y Circulación de esa Información". Con la firma de voces autorizadas del sector se ha sostenido que

6 https://www.oas.org/es/sla/cji/docs/Publicacion_Proteccion_Datos_Personales_Principios_Actualizados_2021.pdf . Una experiencia similar fue del año 2017 para los estados iberoamericanos. En efecto, y a fin de dar cumplimiento a un compromiso asumido en la XXV Cumbre Iberoamericana de Jefes de Estado y de Gobierno, la Red Iberoamericana de Protección de Datos Personales lideró la elaboración de un documento denominado "Estándares de Protección de Datos Personales para los Estados Iberoamericanos" el mismo se encuentra actualmente en etapa de actualización.

> una convención regional de protección de datos puede facilitar e, idealmente, aumentar los estándares de protección de datos en los países participantes, promoviendo la tan necesaria consistencia y coherencia en los marcos regulatorios, reduciendo enormemente la inseguridad jurídica y los costos de cumplimiento para las empresas que operan a través de fronteras, facilitando las transferencias de datos transfronterizas y promoviendo las políticas regionales, integración y crecimiento económico y una digitalización sostenible y cibersegura, contribuyendo al fortalecimiento de la soberanía de cada país miembro.

Y agregan

> La globalización y el creciente intercambio de datos personales entre países de América Latina demandan un marco regulatorio uniforme, que permita proteger la privacidad y los derechos fundamentales de los individuos. Actualmente, existen diversas estructuras jurídicas en la región, como la Organización de los Estados Americanos (OEA), el Pacto Andino y el Mercosur, que podrían albergar dicho acuerdo. De estos, la OEA, con 34 países miembros, ofrece la mayor cobertura y antecedentes en la protección de datos personales y derechos humanos[7].

Tecnologización y habeas data

Desde hace años, vivimos una sociedad hiperconectada en la que los individuos interactúan en un escenario dual compuesto por el mundo real y virtual como uno sólo. Cotidianamente recurrimos a la tecnología para desarrollar innumerables acciones diarias como: comprar, expresarnos, estudiar o trabajar. Esas conductas dejan un rastro personal en la web, exponen datos personales, crean una identidad digital perdurable que traspasa fronteras. Si bien, es cierto que el escenario virtual genera innumerables beneficios también suscita riesgos, amenazas y cuestionamientos respecto a la vigencia de los derechos digitales. Lo cierto es que las fronteras del habeas data, la autodeterminación informativa y los derechos al honor y privacidad se desdibujan.

Basterra (2016) advertía sobre la problemática hace unos años

> Las personas que viven en una sociedad tecnológica desarrollada, a diario proporcionan determinada información acerca de sí mismas, tales como: el domicilio, número de documento, profesión, miembros que integran su familia, si poseen tarjetas de créditos o cuenta bancaria, si tiene automóvil, estudios cursados, datos relacionados con su patrimonio, etc. Toda esta información, es susceptible de ser recopilada en archivos o bancos de datos con la potencialidad de ser utilizada en forma abusiva; con fines discriminatorios o simplemente en forma indebida. Por otra parte, si estos datos se entrecruzan pueden arrojar un

[7] https://cpdp.lat/wp-content/uploads/2024/07/Discussion-paper-CPDP-LatAm-2024.pdf

> perfil completo de la persona, es decir una verdadera "radiografía"; pudiendo significar –según el uso que se les dé- la lesión o cercenamiento de una de las libertades individuales básicas, como es el derecho a la intimidad informática o autodeterminación informativa.

Sibilia (2013) explora el fenómeno de la exhibición en redes sociales de aspectos que antes se consideraban privados. En sintonía con esta idea, Solove (2021) introduce la noción de la paradoja de la privacidad. Esta paradoja describe el comportamiento contradictorio de individuos que, si bien afirman valorar y proteger su intimidad, comparten de forma extensa información personal en línea o aceptan términos y condiciones sin mayor consideración

Es que en efecto, sin desconocer la brecha digital, el Instituto Nacional de Estadísticas y Censos (INDEC) da cuenta de una conectividad creciente. En tal sentido informa para el 4to. trimestre del año 2023, los hogares con acceso a computadora constituyen un 61,0%, los hogares con acceso a internet un 93,4% y que la población que utiliza internet es de un 89,2%[8].

Aún a sabiendas de esta realidad cada vez más compleja, siguen siendo pocas las previsiones en Argentina destinadas a garantizar los derechos digitales. Un ejemplo es la ley 26032 que garantiza el derecho a la libertad de expresión en Internet, también las reformas en materia de cibercrimen acordadas por las leyes 23688 y 26904 que, con ello, revelan cierta tendencia punitivista casi como exclusiva solución al tema[9]. Es decir, no hay legislación relacionada con eventuales responsabilidades de intermediarios, moderación de contenido circulante en la web o mercados digitales para citar algunos de los ejemplos más comunes. Ello genera que las empresas de tecnología -que operan globalmente- impongan sus políticas y condiciones que no siempre son concordantes con los sistemas jurídicos de cada país.

La "Ley Argentina Digital" (ley 27.078) también es relevante en este panorama, ya que establece la competencia del fuero federal para casos relacionados con internet.

[8] Fuente https://www.indec.gob.ar/indec/web/Nivel3-Tema-4-26

[9] El 6 de agosto de 2024 la Comisión de Ciencia y Técnica de la Cámara de Diputados de la Nación llamó a reunión informativa para debatir diversos proyectos sobre inteligencia artificial https://parlamentaria.hcdn.gob.ar/comisiones/reuniones/444/archivo/2HBVBSYDF843P5D4.pdf

Aunque esta interpretación no ha sido aceptada de forma unánime por toda la jurisprudencia, sí es un punto de debate en el ámbito legal[10].

Sintetizando, evidentemente lo digital impuso un cambio profundo y estableció un nuevo paradigma, un diferente modelo social, un cambio en la subjetividad y en los derechos que se agudizó luego de la pandemia del COVID-19. Nuevamente, Sibilia (2013) ya alertaba sobre la exhibición de la privacidad y recuperaba el término "extimidad" como un sentido común que recorre nuestros días.

Como cierre de este análisis elijo referirme a una práctica concreta: las situaciones de vigilancia masiva gubernamental[11] como una conducta que puso en jaque el derecho a la privacidad y fue solo posible por el avance tecnológico.

Las revelaciones realizadas por el ciudadano norteamericano Edward Snowden, ex empleado de la Agencia de Seguridad Nacional (NSA), por vigilancia masiva e ilegal en el marco del programa denominado "PRiSM" constituyen un hito para el mundo occidental dada su magnitud. Estas acciones realizadas por el gobierno estadounidense nacen como consecuencia de los ataques terroristas sufridos por ese país en septiembre del 2001. Un tiempo después, en octubre de ese año se sancionó la "USA Patriot Act"[12] que otorgaba facultades extraordinarias al poder central. Ello habilitó a recopilar correos electrónicos y llamadas de presuntos terroristas. Si bien las medidas debían ser realizadas con autorización judicial, la denuncia dió cuenta de actos masivos contra una innumerable cantidad de personas de todo el mundo, sin intervención judicial y con pruebas lábiles. En este esquema es fundamental destacar la colaboración de parte de empresas de telecomunicaciones estadounidenses como AT&T Inc. y/o multinacionales de tecnología dónde sólo unas pocas empresas como Yahoo y/o Apple pudieron resistirse durante un tiempo ante el atropello[13].

Dicho lo expuesto volviendo a nuestro país, resulta interesante recordar el caso el caso Halabi (CSJN Fallos 332:111). En año 2009 la Corte reafirmó el derecho a la privacidad de las comunicaciones al considerar que ley 25.873 -que pretendía la

[10] Entre otros fallos "Sabores Argentinos S.A. c/Google" -2013-, "Vecchi" -2017-, "Brusco" -2017-, "JL Biautos S.A. c/Vaca Narvaja" -2019-, "Godoy c. Pucheta" -2024.
[11] También hubo otros escándalos como la utilización ilegal del software espía denominado Pegasus (2016) que dejó al descubierto las escuchas y rastreos a mandatarios, periodistas y defensores de derechos humanos, o también el caso en el que se acusó a la consultora Cambridge Analytica (2018).
[12] https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.htm
[13] https://www.dw.com/es/el-gobierno-amenaz%C3%B3-a-yahoo-si-no-colaboraba-con-su-programa-de-espionaje/a-17919145

intervención de las comunicaciones telefónicas y por Internet de manera genérica e imprecisa- violaba garantías constitucionales[14]. Además, la jurisprudencia señaló el reconocimiento de las "acciones de clase" como una herramienta destinada a proteger derechos iguales. Ello supone que la sentencia tenga efectos para todos los ciudadanos que comparten un idéntico problema.

Del mismo caso me interesa subrayar un argumento expuesto por el reclamante y es su condición de "consumidor". La apelación a esa rama del derecho es una cuestión cada vez más común en discusiones relativas a la protección de datos personales con el objetivo de fortalecer el derecho a la protección de datos personales. Ello se observa en dos casos de reciente trascendencia pública. El primero del año pasado, se dió frente a la irrupción de la empresa "Worldcoin" cuyo objeto es desarrollar una criptomoneda y brindar una identidad digital mundial mediante el escaneo del iris[15]. También unos años antes, en el año 2021 en momentos de discutir los cambios en las condiciones y políticas del sistema de mensajería instantánea de Meta "Whatsapp" intervino la Comisión Nacional de Defensa de la Competencia quien aplicó multas a la empresa[16].

En resumen, si bien en nuestro país, el caso Halabi consideró que las comunicaciones integran la esfera de intimidad personal y se encuentran alcanzadas por las máximas protecciones constitucionales no podemos negar que ante el avance tecnológico la recopilación de información para perfilamiento o el acceso de datos personales sin consentimiento se vuelve una posibilidad.

Conclusiones

El hábeas data es una herramienta jurídica fundamental para la protección de los derechos personalísimos como la intimidad y el honor de las personas, valores esenciales en las sociedades democráticas. Sin embargo, su eficacia se ve comprometida por la rápida evolución tecnológica, que ha puesto en cuestión sus límites y en crisis su capacidad para garantizar de manera adecuada el derecho a la privacidad. La transformación social ha

[14] https://www.argentina.gob.ar/noticias/nuevas-condiciones-del-servicio-y-politicas-de-privacidad-de-whatsapp-0

[15] https://www.gba.gob.ar/produccion/noticias/la_provincia_sancion%C3%B3_worldcoin_con_una_multa_de_194_millones

[16] https://www.argentina.gob.ar/noticias/nuevas-condiciones-del-servicio-y-politicas-de-privacidad-de-whatsapp-0

redefinido el concepto de "ser dejado a solas", exigiendo una revisión de su marco normativo que acompañe el nuevo estado de situación.

Por ello, resulta imperativo impulsar una actualización legislativa que responda a los desafíos del entorno digital. Asimismo, es crucial fomentar un Estado sólido, innovador y proactivo, capaz de anticiparse a los cambios y garantizar la protección de los derechos individuales. El sector empresarial también debe asumir un papel activo, comprometiéndose con una innovación responsable, que priorice el respeto a los derechos humanos.

En este proceso de adaptación, es esencial preservar los principios y valores que sustentan nuestro ordenamiento jurídico, evitando que los avances tecnológicos socaven los derechos individuales y debiliten las instituciones democráticas

Referencias bibliográficas

Banisar, D. (2024). *National Comprehensive Data Protection/Privacy Laws and Bills 2024*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1951416

Basterra, M. (2016). *Habeas Data: Los Derechos Protegidos*. https://marcelabasterra.com.ar/wp-content/uploads/2016/11/HD.-Habeas-Data.-Derechos-Protegidos.-Marcela-I.-Basterra.-03.3.10.pdf

Sibilia, P. (2013). *La intimidad como espectáculo*. Fondo de Cultura Económica.

Solove, D. J. (2021) The Myth of the Privacy Paradox. *George Washington Law Review.* 89 (1). http://dx.doi.org/10.2139/ssrn.3536265