REVISTA CHILENA
DE DERECHO Y TECNOLOGÍA

VOL. 14 (2025) • e73836 • DOI 10.5354/0719-2584.2025.73836
RECIBIDO: 2/2/2024 • APROBADO: 10/6/2025 • PUBLICADO: 31/12/2025

DOCTRINA

Una investigación empírica de la cultura de protección de datos personales y la actuación de las autoridades nacionales en Latinoamérica

Empirical research of data protection culture and the national authorities' role in Latin America

Alexandre Veronese **Rebecca Lemos Igreja** **Marcio Iorio Aranha**
Amanda Nunes Lopes Espiñeira Lemos **Mariana Moutinho Fonseca**
Luiza Mendonça da Silva Belo Santos **Luiza Veiga**
Amanda Braga Ferreira **Vitória Sernégio**
Universidad de Brasilia, Brasil

Alessandra Silveira
Universidade do Minho, Portugal

Thiago Guimarães Moraes
Laboratorio de Políticas Públicas e Internet, Brasil

Eduarda Costa
Centro de Direito, Internet e Sociedade, Brasil

RESUMEN Este artículo presenta los resultados de una investigación de campo sobre autoridades de protección de datos personales en ocho países de Latinoamérica y analiza el fortalecimiento de la cultura de protección de datos en la región. El trabajo describe perspectivas nacionales y regionales. La protección de datos personales, como derecho, a pesar de tener un carácter global, posee narrativas locales que forman la cultura de protección de datos de cada país y las interpretaciones normativas para regular el tema. Las autoridades, la sociedad civil y los demás actores involucrados reflejan esas especificidades y la influencia existente de otros países. La conclusión del artículo es que el concepto jurídico de protección de datos personales tiene un conocido contorno internacional, pero gana interpretaciones locales en Latinoamérica, con un grado de interacción entre los países de la región.

PALABRAS CLAVE Protección de datos, privacidad, autoridades, Latinoamérica, políticas públicas.

ABSTRACT This paper presents the analysis of the results of a fieldwork investigation on personal data protection authorities in eight countries of Latin America and the strengthening of data protection culture in this region. The work describes national and regional perspectives. Personal data protection as a right, despite having a global nature, has local narratives that shape the data protection culture of each country and the interpretations of norms and standards to regulate the subject. The role of data protection authorities, civil society actors, and other players reflect these specificities and the existing influence of other countries. The conclusion of the article is that the global concept of personal data protection has a well-known international framework. Nonetheless, this global concept gains local interpretations in various Latin American countries, with a degree of interaction between them.

KEYWORDS Data protection, privacy, authorities, Latin America, public policies.

Introducción

Este artículo aborda conclusiones derivadas de investigaciones de campo, en las que se incluyen entrevistas a autoridades, académicos y representantes de la sociedad civil. También contempla el análisis bibliográfico, documental y de legislación comparada del «Proyecto de investigación documental y de campo sobre autoridades de protección de datos en América Latina: El concepto social e institucional de privacidad y datos personales» de la Fundación de Apoyo a la Investigación del Estado de São Paulo.[1] El objetivo de la investigación es comprender cómo ha sido planteada en las culturas jurídicas nacionales de los países latinoamericanos la noción de protección de la privacidad y de datos personales. El uso de entrevistas, doctrina jurídica, juzgados y fuentes documentales lo cualifica como una pesquisa jurídica y social. Si el lector hace una lectura crítica verá que incluso opiniones impresas en libros pueden contener puntos de vista muy distintos a la realidad. Así, utilizar múltiples fuentes como metodología de investigación (incluidas aquellas de personas que no son profesores de derecho) es una forma de conocer visiones sobre temas jurídicos por vías más amplias (Schuck, 1999).

En este trabajo se revisan de modo amplio las herramientas teóricas que permitieron el análisis en cuestión. Así, se indica que el concepto de cultura jurídica para la protección de la privacidad y de los datos personales solo puede entenderse por la

1. Más información del proyecto se puede encontrar en «Documentary and field research on the Latin American data protection authorities: The social and institutional concept of privacy and personal data», *fapesp.br*, disponible en https://tipg.link/lA66.

conjunción de dos perspectivas. La primera se refiere a hechos y actos —retirados de documentos, entrevistas, informes y productos— que fundamentan la construcción sociocultural alrededor del tema y que se traducen en una subcultura jurídica. Los factores que los fundamentan varían según el país y pueden reflejarse en demandas económicas de inserción al mercado global o en la lucha por la modernización de las leyes, como defiende la sociedad civil organizada en algunos países. Sin embargo, esos factores nunca están aislados. Lo que unifica a todos los países es la necesidad de alcanzar un mínimo consenso social para que se puedan modificar las leyes y pueda tener lugar la creación de institutos jurídicos.

Además de esa perspectiva estructural, hay una segunda que contempla procesos sociales más específicos y peculiares, que pueden organizarse en mediaciones. Las mediaciones constituyen un proceso de traducción local por parte de distintos grupos sociales de instituciones externas e internas, ya sean del Estado, del mundo académico o de la sociedad civil (Choudhry, 2006: 29).

La primera sección de este artículo está dirigida a identificar elementos discursivos que señalan la universalidad del debate, especialmente en la traducción de elementos. El foco es el interés de las instituciones latinoamericanas en adecuarse a los parámetros universales de modernidad jurídica y social, movilizando discursos sobre derechos humanos y constitucionales. Se demostrará cómo ciertos casos judiciales han sido fundamentales para la construcción de esas narrativas y para la traducción de soluciones procesales como el *habeas data*. Por ejemplo, en Perú, el Tribunal Constitucional delineó los distintos tipos de *habeas data* vigentes en el ordenamiento jurídico del país en una citada «sentencia académica» (Pucccinelli, 2020: 26).

La segunda sección compara discursos y narrativas sobre las influencias de los modelos y prácticas de algunos países sobre otros, específicamente en América Latina. La tercera sección aborda las dificultades para comprender los derechos de los interesados en los países entrevistados. La sección plantea los factores que se consideran obstáculos para el desarrollo del derecho a la protección de la privacidad y de los datos personales. La cuarta sección se centra en temas cruciales para la conclusión, que se refieren a las interacciones e intercambios entre los distintos países. Allí, se aborda las influencias de los países latinoamericanos entre sí como una especie de embrión de una cultura jurídica regional en materia de protección de datos personales y el papel de la Red Iberoamericana de Protección de Datos en ese proceso.

La conclusión del artículo es que existen elementos culturales e institucionales que clarifican interacciones entre muchos países de Latinoamérica sobre ese tema. Así, es posible tener en cuenta un proceso social más amplio de construcción de una tipología plural con aportes universales y con traducciones locales del derecho a la protección de datos personales.

Contraste de los países encuestados por creencias, hechos y procederes relevantes para la construcción de la cultura de protección de datos personales y privacidad

El derecho es una construcción social muy compleja que implica grados de discursos sociales (Restrepo, 2012). Comprender, en armonía con la isonomía, un amplio conjunto de discursos, emanados de varios actores (funcionarios del Estado, empleados de las autoridades de control, docentes, investigadores, activistas, entre otros), es ver cómo se construyen los derechos en lo cotidiano. El análisis transversal de esos discursos muestra cómo se han erigido los derechos a la protección de datos personales y a la privacidad en diversos contextos socioculturales, mientras se desarrolla algo potencialmente universal (Doneda, 2006). A lo largo de las entrevistas que sirven de base a este estudio, en varios países se percibe la construcción narrativa de la legitimidad de tales derechos, en tanto se describen ya sea como derechos humanos o como derechos constitucionales o derechos fundamentales (Álvarez Robles, 2022: 15).

Apreciar los fenómenos culturales y sus relaciones entre los diversos actores sociales es un enorme desafío. Cabe señalar que se ha prestado atención a la hipótesis de que no existe uniformidad nacional en esa cuestión, puesto que los discursos sobre derechos siempre tienen una pluralidad de interpretaciones y comprensiones.

Discursos a favor de la universalidad cultural, la privacidad y la protección de datos personales

El primer dilema que emerge del análisis de los países que están con la agenda de la protección de datos personales y el derecho a la privacidad es el establecimiento de un paralelismo entre varias narrativas culturales de dimensión universal y su implementación local.

Los derechos humanos, constitucionales o fundamentales como reflejo de la universalidad

Un elemento diferenciador de América Latina es la construcción constitucional y legal del *habeas data* como instrumento para la protección de la información y, posteriormente, para la protección de los datos personales y la privacidad. Un primer ejemplo es el caso de Perú. En la Constitución Política de 1993, el *habeas data* está previsto en los artículos 200 y 202. Como bien lo explican las entrevistas, se percibe como un derecho constitucional de acción que no requiere el agotamiento de los recursos administrativos (Veronese y otros, 2023a: 497). Esa explicación queda clara en la presentación realizada en la entrevista a la autoridad de protección de datos del país. Allí, la entrevistada explica que esa vía procesal está relacionada con el derecho a la información y a la transparencia, a la vez que le añade el derecho a la protección

de datos personales y a la autodeterminación informativa (Veronese y otros, 2023a: 530).

Una entrevistada de la sociedad civil indicó enfáticamente que el origen del *habeas data* se refería al acceso a la información y a la transparencia, sin considerar la ampliación del instrumento de protección de datos personales (Veronese y otros, 2023a: 531). Además, una entrevistada del sector empresarial señaló que existen dos caminos para la protección de los datos personales y la privacidad. El primero es el *habeas data* y el segundo, en sus términos, es la vía administrativa (Veronese y otros, 2023a: 507).

La jurisprudencia de la Corte Constitucional de Perú es evidente en la construcción del vínculo directo entre los documentos de derecho internacional y la resolución de cuestiones de aplicación de *habeas data*. En el caso *Genaro Villegas Namuche*, la Corte invocó el Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas, así como la Convención Americana sobre Derechos Humanos (Pacto de San José de Costa Rica) de la Organización de los Estados Americanos, en su párrafo 5.[2] No obstante, esa interpretación podría seguir otro camino, ya que, según una entrevistada de la sociedad civil peruana, el artículo 2.6 de la Constitución Política de 1993 establece como derecho fundamental la protección de la información personal en los sistemas informáticos (Veronese y otros, 2023a: 454).

En cuanto a la declaración de esta última entrevistada, es evidente que el lapso mencionado, de 1993 a 2012, computa la inclusión del periodo de *vacatio legis* de la Ley 29733/2011, que menciona explícitamente la reglamentación del artículo 2.6 de la Constitución Política. Ese punto de vista es corroborado por la opinión de una entrevistada de la sociedad civil que, asertivamente, enfatiza la constitucionalización del derecho a la protección de datos personales en Perú, a pesar de que no se encuentra expresado directamente en la Constitución Política. Ese razonamiento es lógico, ya que verifica que la propia Ley 29733 trae una referencia directa al texto constitucional, como explica también un entrevistado de la sociedad civil (Veronese y otros, 2023a: 454). Cabe recordar que el caso resuelto por el Tribunal Constitucional del Perú, mencionado anteriormente, es de 2004, lo que complejizaría la construcción jurídica: Constitución, ley, órgano administrativo y decisiones judiciales.

Es evidente que se trata de una construcción social e interpretativa de la ley, como ocurrió en varios otros países de la región, incluido Brasil, antes de la Enmienda Constitucional 115 de 2022. Esas narrativas y hechos evidencian los intentos de construir discursos sociales y jurídicos a favor de la universalidad de los derechos a la información, de la transparencia y, más recientemente, de la protección de datos personales en Perú.

2. Sentencia del caso *Genaro Villegas Namuche,* Tribunal Constitucional de Perú, recurso extraordinario 2488-2002-HC-T, 18 de marzo de 2004, disponible en https://tipg.link/kv6n.

La misma dinámica de mediación cultural es visible en Costa Rica. La Constitución Política de la República de Costa Rica, del 7 de noviembre de 1949, trata el derecho a la privacidad en el artículo 24 y en el artículo 28. Así, aunque no exista una disposición expresa para proteger datos personales, el intento de anclar ese derecho en el ámbito constitucional es claro (Veronese y otros, 2023b: 858). Ese camino narrativo e interpretativo alcanza también a la construcción de medios procesales de defensa. Ni la Constitución Política de 1949 ni ninguna reforma o ley posterior creó el *habeas data* como un medio procesal específico. Según una entrevista a la autoridad de protección de datos del país, aunque no existe una regulación del *habeas data*, varias personas utilizan esa expresión para referirse al recurso de amparo, un medio procesal correcto utilizado para postular la protección de datos personales, con foco en el artículo 24 de la Constitución (Veronese y otros, 2023b: 926). A pesar de la visión técnica y especializada de que la acción judicial no es un *habeas data*, es evidente que parte del imaginario social utiliza esa expresión para referirse a un derecho de acción para la protección de datos personales, como lo explica una entrevistada del sector empresarial (Veronese y otros, 2023b: 875).

Colombia es otro ejemplo de esa práctica. El texto constitucional de Colombia es de 1991 y las entrevistadas recurrirán a los artículos 15 y 20, en su redacción original, para derivar la construcción de un derecho a la protección de datos personales. Como la Constitución Política de Perú, el texto constitucional colombiano ha hecho previsión de recursos informáticos. Resalta que el texto alude directamente a la recolección, al procesamiento y a la circulación de datos, como explica Nelson Remolina Angarita (2015: 121). Esto ocurre debido al trabajo de una comisión preparatoria, que anticipó la necesidad de incluir los medios tecnológicos contemporáneos de la época en la que se estaba construyendo el texto. Además, en las comisiones también se construyó el debate sobre el *habeas data*, así como discusiones sobre los fundamentos de los derechos que se deben reconocer, como explica el mismo autor (Remolina Angarita, 2015).

El texto constitucional colombiano tampoco hace alusión directa al *habeas data* como medio procesal específico. Fue una construcción legislativa la que luego reguló ese instituto mediante la Ley 1266 de 2008, que se refiere explícitamente a los artículos 15 y 20 de la Constitución, en su artículo 1 (Cervantes Díaz, 2009). Esa construcción tuvo evidentes efectos prácticos, ya que permitió el empleo de la acción de tutel. Por medio de esa acción, se abrió un canal para revisar las sentencias de los tribunales inferiores directamente por la Corte Constitucional, incluso en casos de *habeas data*, según explicó una académica entrevistada (Veronese y otros, 2023b: 1040). Además, esa construcción se ha vuelto más sólida debido a la separación entre el derecho a la privacidad y a la protección de datos personales, por medio de una decisión judicial del Tribunal Constitucional, tal y como explica el entrevistado de la autoridad de protección de datos (Veronese y otros, 2023b: 991).

Por su parte, la Constitución de la República de Chile, que data de 1980, incluyó el derecho a la protección de datos personales de manera expresa en el artículo 19 número 4, mediante una reforma constitucional en 2018 (Contreras Vásquez, 2020), aunque había ya una preocupación antigua sobre el tema (Arrieta Cortés, 2009). Estudios como el de Carlos Reusser Monsálvez (2021: 145) mencionan que, en el Poder Judicial chileno, de igual modo que en otros países de la región, se dio el uso de disposiciones constitucionales de protección de la vida privada para atender casos de protección de datos personales. Sin embargo, en Chile destaca la falta de una disposición expresa sobre el derecho al olvido (Contreras Vásquez, Bordachar Benoit y Ortiz Mesías, 2022: 77).

Hay una colección de jurisprudencias que evidencia cómo esas disposiciones constitucionales han servido de punto de partida para importantes decisiones, como el uso de bases de datos por la agencia nacional de inteligencia, la protección de datos de personas condenadas, la vigilancia de correos electrónicos de funcionarios y el uso del dominio público (Contreras Vásquez, Bordachar Benoit y Ortiz Mesías, 2022). Cuando Chile discutía su revisión constitucional, los profesores Álvarez-Valenzuela y Zaror Miralles (2022) propusieron que la nueva carta hiciera hincapié en el ejercicio de los derechos fundamentales en la red (derechos digitales), incluyendo la protección de los derechos, la protección de los datos personales y la ciberseguridad

Chile es un caso especial, ya que tiene una disposición constitucional expresa para el derecho a la protección de datos personales. Sin embargo, el Consejo para la Transparencia ha asumido el rol de regulador administrativo de temas relacionados con privacidad, protección de datos y ciberseguridad en el país, pero solamente direccionados al sector público (Benussi Díaz, 2020). La otra vía posible es la judicial, pero una de las entrevistadas de la sociedad civil se muestra escéptica sobre la interpretación que el Poder Judicial pueda dar a ese derecho (Veronese y otros, 2023b: 1213). Ese contexto de transformaciones ha repercutido y permitió que Chile discutiera la necesidad de actualizar la Ley 19628, del 28 de agosto de 1999, a partir de un proyecto de ley de 2017, que ya está en trámite.[3]

Es importante señalar tres puntos que se han dispuesto como centrales de la nueva ley. El primero es la construcción de una autoridad administrativa para la protección de datos personales, el segundo es la interiorización de las normas legales que regulan las transferencias internacionales de datos personales y el tercero es la construcción de un sistema de eficacia. Durante el proceso legislativo se plantearon puntos de mejora en la propuesta legislativa, como una mayor protección de los derechos de acceso, rectificación, cancelación y oposición. Por ejemplo, se planteó la necesidad

3. Senado de la República Chile, «Protección y tratamiento de datos personales: claves de la modernización en trámite», *senado.cl,* disponible en https://tipg.link/l-LB.

de incluir un derecho de oposición que aborde el procesamiento de datos basado en el interés público o el interés legítimo de los individuos (Bordachar Benoit, 2022).

El caso de Brasil tiene una similitud con Panamá. Ambos países cuentan con marcos legales específicos bastante recientes para la protección de datos personales (del 2018 en el caso de Brasil y del 2019 en el caso de Panamá). Sin embargo, al igual que en otros países de la región, es evidente el uso del *habeas data* como un medio para enfrentar el tema. Brasil fue el primer país de América del Sur y el Caribe en prever ese remedio en su Constitución Federal de 1988 (Doneda, 2006: 326). Sin embargo, como ocurrió en los demás países investigados, ese medio legal por sí solo no fue suficiente para garantizar la protección de los datos personales por medio de la interpretación judicial.

La puesta en vigencia de la Ley 13709/2018, así como su rápida modificación, fue necesaria para crear la Autoridad Nacional de Protección de Datos (ANPD). Se observa en Brasil que el derecho a la protección de datos personales deriva de los derechos fundamentales de la personalidad y de la protección de la privacidad. El mayor ejemplo es el juicio conjunto de varias acciones constitucionales (6387, 6388, 6389, 6390 y 6393). Esa sentencia, medida cautelar refrendada por el Pleno del Supremo Tribunal Federal, reconoció la existencia del derecho fundamental a la protección de datos personales en los siguientes términos:

> Como resultado de los derechos de la personalidad, se afirmó el respeto a la privacidad y la autodeterminación informativa, en el artículo 2, I y II, de la Ley 13709/2018 (Ley General de Protección de Datos Personales), como fundamentos específicos de la disciplina de la protección de datos personales.[4]

Como en el debate se trató la medida relacionada con el abordaje de la crisis sanitaria mundial del covid-19, el tribunal también mencionó documentos de la Organización Mundial de la Salud para respaldar su decisión de declarar inconstitucional la Medida Provisional 954/2020. Luego, en 2022, el Congreso Nacional aprobó la mencionada enmienda constitucional y, así, el derecho a la protección de datos personales adquirió carácter explícito en el texto constitucional brasileño (Mendes y Da Fonseca, 2020).[5]

Veamos ahora el caso de Argentina, cuya constitución se remonta a 1853, con amplias modificaciones. El texto constitucional se ha modificado mucho, en especial en 1994. Una de estas modificaciones a la redacción —sobre la versión 1957— fue la

4. Referendo na Medida Cautelar na Ação Direta de Inconstitucional 6.388 Distrito Federal, Supremo Tribunal Federal de Brasil, 7 de mayo de 2020, disponible en https://tipg.link/k-V4.

5. Para más información sobre la enmienda, véase Cámara de Diputados de Brasil, «Comissão Especial destinada a proferir parecer à Proposta de Emenda à Constituição n. 17. 2019», disponible en https://tipg.link/l9_W.

introducción de artículo 43 inciso tercero, que disponía el *habeas data* bajo el epígrafe general de la acción de amparo (Puccinelli, 2014). Como explica Pablo Palazzi (1998), ese camino hacia el *habeas data* no fue sencillo, ya que la Presidencia vetó la Ley 24475/1996, que había sido aprobada por el Congreso de la Nación. A pesar de ello, según un entrevistado del área académica, eso no impidió que el Poder Judicial lo empleara a favor del acceso a la información (Veronese y otros, 2023b: 1345).

Es importante señalar que la autonomía del *habeas data*, en relación con el juicio de amparo, fue un proceso básico para ampliar el alcance de ese recurso a favor de la protección de datos personales (Palazzi, 1998). Según un entrevistado del Gobierno argentino, el juicio de amparo sería similar al procedimiento de *mandado de segurança* (mandato de seguridad) en la legislación brasileña (Veronese y otros, 2023b: 1300). Como se puede observar en el tercer inciso del artículo 43, el *habeas data*, en Argentina, también puede ser presentado contra bases de datos privadas.

Recurrir al Poder Judicial para la protección de datos personales fue una práctica recurrente en Argentina entre 1994 y 2000 (Veronese y otros, 2023b: 1275). La Ley 25326/2000, que trata de la protección de datos personales, introdujo un capítulo específico sobre el *habeas data*, con lo que se dio solución al dilema inicial. El proceso de interpretación constitucional obtuvo su primer fallo importante en ese periodo por parte de la Corte Suprema en el caso *Facundo Urteaga*, en el que se garantizó el *habeas data* como extensión del derecho a la privacidad (Ruiz Martínez, 2015: 61).[6] Según uno de los entrevistados, ese caso generó una gran conmoción social (Veronese y otros, 2023b: 1283), en tanto la Corte Suprema terminó permitiendo el acceso a los datos personales de una persona desaparecida, tal y como lo había solicitado su hermano.

Según Marcela Basterra (2008a: 68), el caso *Facundo Urteaga* está también directamente relacionado con el debate sobre el derecho a la verdad. En la misma línea que la opinión de esa autora, el derecho a la protección de datos personales se entiende como un derecho de acceso a otros derechos fundamentales, como explica una entrevistada de la sociedad civil (Veronese y otros, 2023b: 1407). En un sentido similar, una entrevistada del Gobierno señala que el derecho a la protección de datos personales es un «derecho intermedio» y lo considera un medio para proteger otros derechos fundamentales (Veronese y otros, 2023b: 1310).

Un dato curioso es que Argentina fue uno de los países que más tardó en incorporar el derecho de acceso a la información pública en América Latina: su Ley de Acceso a la Información (Ley 27275) es de 2016. El asunto no estaba en un vacío legal, pues la Constitución ya contemplaba derechos relacionados con el tema y también lo hacían un ente derivado de la Ley 25326/2000 (la Dirección Nacional de Protección

6. Sentencia del caso *Urteaga, Facundo Raúl c/ Estado Nacional*, Corte Suprema de Justicia de la Nación Argentina, número interno U14XXXIII, 15 de octubre de 1998, disponible en https://tipg.link/k-dO.

de Datos Personales) y el Decreto 1172/2003 (Veronese y otros, 2023b: 1345). El advenimiento de la Ley 27175 fue importante para combinar administrativamente el sistema. Esa ley creó la Agencia de Acceso a la Información Pública como un organismo autárquico, incorporando a la Dirección Nacional de Protección de Datos Personales (Simão, Oms y Torres, 2019: 12).

El caso de Argentina también demuestra una construcción interpretativa y la influencia de elementos internacionales para la delimitación del concepto y de los instrumentos locales orientados a proteger los datos personales. Uno de los problemas de la región es el equilibrio entre la protección de datos personales y el deber constitucional de transparencia, situación que se repite en varios países, como en Chile, Panamá y México.

En el caso de México, la entrevista a una autoridad del país señala esa dificultad a partir de que en el año 2000 se había producido una amplia reforma institucional para el tema del acceso a la información, que como consecuencia se había entrelazado con el tema de la protección de datos personales y la privacidad. Los gestores se habían preguntado «¿cuál sería la condición de la información de los ciudadanos?». La respuesta fue la necesidad de construir un marco normativo e institucional para la protección de los datos personales y la privacidad, influenciado por fuentes internacionales y definiéndose que la competencia para la materia sería federal (Veronese y otros, 2023a: 788).

Ese marco inicial cobró una nueva dimensión con la reforma a la Constitución Política de 2009, que reconoció la autonomía del derecho a la protección de datos personales en relación con el derecho de acceso a la información (Parra Noriega, 2011: 155). La influencia regional (es decir, del debate latinoamericano) es evidente cuando se observa que el texto constitucional mexicano prevé los derechos de acceso, rectificación, cancelación y oposición (Veronese y otros, 2023a: 630). Así, la influencia internacional en la incorporación constitucional de los derechos a la protección de datos personales en México es clara, en línea con un proceso social en curso en los distintos países de América Latina.

El camino de Uruguay fue algo diferente, ya que esos derechos no estaban expresamente incluidos en su texto constitucional. A la fecha, el anclaje constitucional de esos derechos en el país se lleva a cabo por el artículo 72 de la Constitución, que los vincula a los derechos de la personalidad. En Panamá, por su parte, tanto la doctrina nacional como el Poder Judicial derivan el derecho constitucional a la protección de datos personales de los derechos a la privacidad e intimidad (López Carballo y González Calero-Manzanares, 2015: 152-155).

En este sentido, si se tienen en cuenta los panoramas nacionales y su relación con el derecho internacional es posible identificar en los países investigados la existencia de una dinámica social y jurídica de producción de derechos fundamentales o constitucionales. No obstante, la visión descrita en este subapartado pone de manifiesto

una producción cultural de internalización de diversos elementos externos en textos y narrativas locales. La siguiente subsección tratará un tema relacionado con ello. Sin embargo, estará más atenta a las prácticas, especialmente cuando se refieran a la necesidad de modernizar las estructuras jurídicas de los países.

Los derechos y las prácticas nacionales como reflejo de una modernidad jurídica global, aunque occidental

En las entrevistas que sirven de base a esta investigación, se percibió que había, en las narrativas, un sentido de la necesidad de insertar a los países investigados en un paradigma de modernidad jurídica. En vista a ello, la atención en esta subsección se centrará en analizar los casos judiciales o administrativos y los discursos pronunciados, siempre bajo la perspectiva de la inserción internacional y transnacional de los países.

Perú aporta un primer ejemplo en una decisión administrativa de 2015 sobre el «derecho al olvido».[7] Fue una decisión contra Google con el objetivo de borrar enlaces. La primera pregunta es si esta decisión está relacionada con el caso resuelto por el Tribunal de Justicia de la Unión Europea conocido como *Mario Costeja*.[8] En este caso, el tribunal determinó que existiría un derecho individual contra Google para eliminar un enlace difamatorio, sin eliminar el texto de Internet. En resumen, ambos casos tratan la misma cuestión jurídica. El «derecho al olvido» ha despertado la curiosidad de la población y del mundo jurídico en general sobre la protección de datos personales y la privacidad. Con todo, el resultado de las sentencias y decisiones administrativas latinoamericanas en las que se utiliza esa expresión puede diferir mucho del que se construyó en la Unión Europea. En el caso peruano, la Ley 29733 de 2011 no contempla expresamente el derecho al olvido («desindexación», en el sentido de la Unión Europea), aunque en su artículo 20 sí aborda los derechos de actualización, inclusión, rectificación y supresión. Sin embargo, eso no fue obstáculo para que la Dirección Nacional de Protección de Datos Personales del Perú decidiera administrativamente sobre el tema, determinando la desindexación de enlaces por parte de Google en el caso analizado.[9]

Esta decisión administrativa es mencionada por un entrevistado de la sociedad civil como un hecho crucial para la conformación de la autoridad de protección de datos del país desde 2015 (Veronese y otros, 2023a: 471) y la relaciona explícitamente

7. Resolución Directoral 045-2015-JUS/DGPDP, Dirección General de Protección de Datos Personales, Perú, 30 de diciembre de 2015, disponible en https://tipg.link/l-Lf.

8. Sentencia del Tribunal de Justicia (Gran Sala) de la Unión Europea, asunto C131/12, 13 de mayo de 2014, disponible en https://tipg.link/l-Lq.

9. Martin Borgioli, «Google es sancionado por primera vez en Perú por desconocer el derecho al olvido», *Hiperderecho*, 21 junio de 2016, disponible en https://tipg.link/k-q6.

con el caso *Mario Costeja*. El caso peruano fue importante porque demostró que la autoridad local podía sancionar a una empresa global, tal como se hizo en la Unión Europea. Recientemente, la Corte Constitucional decidió de manera similar.[10]

En Costa Rica, encontramos dos casos que abordan el tema. Aunque son locales, muestran el mismo sentido de que la aplicación de sanciones sirve para visibilizar el problema y para demostrar que las autoridades locales cumplen las prácticas de otros países. El primero se conoce como caso *UPAD*, siglas de de la Unidad Presidencial de Análisis de Datos, un organismo directamente adscrito a la Presidencia de la República de Costa Rica, según explicó una de las entrevistadas de la sociedad civil. Ese órgano fue creado por decreto y marcó un antes y un después en el debate costarricense (Veronese y otros, 2023b: 838). Otra entrevistada de la sociedad civil explicó que esa unidad se creó para analizar masivos datos personales de los ciudadanos y producir políticas públicas más eficientes (Veronese y otros, 2023b: 820), lo que preocupó mucho a la ciudadanía. La propia Presidencia de la República revocó el decreto de creación de la UPAD, pero esto no hizo que el problema desapareciera. Diversos grupos políticos, autoridades estatales y entidades de la sociedad civil se han movilizado en ese sentido.[11] De hecho, aún está pendiente una demanda judicial sobre el caso.[12]

El segundo es el caso de las pruebas Faro, relacionado con la recolección de datos personales por medio de un cuestionario entregado a niños en exámenes periódicos realizados en el país, como se puede leer en un artículo periodístico.[13] Una entrevistada de la sociedad civil costarricense explicó que esas pruebas se aplicaban a estudiantes de once años. Sin embargo, había preguntas que eran de carácter socioeconómico. Esas preguntas, según la entrevistada, habrían generado un trauma en los niños, lo que llevó a un sentimiento de indignación entre los padres de los estudiantes (Veronese y otros, 2023b: 841). Curiosamente, ambos casos se relacionan con el propio Estado, a diferencia del caso contra Google en Perú.

El tema de la modernización legal para amparar la protección de datos personales también ha avanzado significativamente por medio de decisiones judiciales y administrativas en Colombia. El enfoque del día a día del trabajo de la autoridad de protección de datos en ese país está relacionado con temas financieros, como el otorgamiento de créditos, según uno de los entrevistados de la entidad (Veronese y otros, 2023b: 982). El profesor Rodrigo Flórez Ruiz afirma que la Corte Constitu-

10. Véase la sentencia del caso *Miguel Arévalo Ramírez contra Google Perú SRL y otros*, Tribunal Constitucional de Perú, rol 199/2022, 17 de junio de 2022, disponible en https://tipg.link/k-qF.

11. Tomás Gómez, «A un año de histórico allanamiento: 10 momentos clave del caso UPAD», *El Observador*, 1 de marzo de 2021, disponible en https://tipg.link/loRA.

12. Tomás Gómez «Caso UPAD: Estas son las penas a los delitos que la Fiscalía acusa al presidente Alvarado», *El Observador*, 4 de febrero de 2022, disponible en https://tipg.link/loRC.

13. Tomás Gómez, «Pruebas FARO costaron 2.319 millones: 11% fue por polémicos cuestionarios de datos personales», *El Observador*, 16 de noviembre de 2021, disponible en https://tipg.link/loRL.

cional colombiana, en la sentencia T-414/92, habría adoptado una forma fuerte de interpretación de los datos financieros, de modo que estuvieran protegidos por el derecho a la privacidad. En consecuencia, su disponibilidad solo sería posible con el consentimiento del interesado. Un dato negativo debería ser rechazado tan pronto como se pagase la deuda (Flórez Ruiz, 2011: 83).

La Corte Constitucional de Colombia ha establecido estándares para la exposición o protección de los datos personales de las personas (De la Calle Restrepo, 2009: 53). Entre 2008 y 2013 produjo decisiones consolidando varios entendimientos, como la definición de un «derecho de libre determinación de la información digital» en la sentencia T-094 de 1995,[14] concepto que es repetido en la sentencia T-729 de 2002 (De la Calle Restrepo, 2009: 47).[15] En ese sentido, Betsy Ruiz Ardila (2016: 33), en su monografía, considera que la protección de datos personales combina varias fuentes, entre ellas la Corte Constitucional y la Superintendencia de Industria y Comercio (SIC). Esa entidad incluso aporta sentencias en las que basar sus decisiones (Veronese y otros, 2023b: 1095). La producción de conceptos jurídicos renovados, en un diálogo jurídico entre el Poder Judicial y las autoridades administrativas, demuestra el énfasis que se le da en Colombia a la necesidad de participar en un proceso local de modernización jurídica con una mirada más allá de sus fronteras.

Como ya se mencionó, Chile no cuenta aún con una autoridad dedicada de modo exclusivo a la protección de datos personales. En términos prácticos, el Consejo para la Transparencia ha sido el principal responsable de la protección de datos, así como del acceso a la información pública. Como se señaló en la subsección anterior, Chile se encuentra debatiendo la reformulación de su legislación específica, centrándose en esos temas. Esa discusión habría comenzado en 2014, pero el proyecto recién se presentó en 2017 (Veronese y otros, 2023b: 1187).

Existen factores internacionales que justificarían la actualización del sistema administrativo y legal chileno, conforme demuestran las entrevistas realizadas. El primero es la participación en la Cooperación Económica Asia-Pacífico (APEC, por sus siglas en inglés) (Veronese y otros, 2023b: 1165 y 1246). Además, Chile es parte del Digital Economy Partnership Agreement, un tratado que implica la flexibilidad de los flujos de datos personales entre sus miembros (Nueva Zelanda, Chile y Singapur) (Veronese y otros, 2023b: 1193).

Ese enfoque hacia el Pacífico distingue a Chile de otros países latinoamericanos. Así, los entrevistados mencionaron poca influencia del derecho comparado en los

14. Sentencia del caso *Carlos Alberto Legarda Valencia contra la Asociación Bancaria y entidades financieras*, Corte Constitucional de Colombia, rol T-094, disponible en https://tipg.link/lA30.

15. Sentencia del caso *Carlos Antonio Ruiz Gómez contra Departamento Administrativo de Catastro de Bogotá y por la Superintendencia Nacional en Salud*, Corte Constitucional de Colombia, rol T-729, disponible en https://tipg.link/l-Ly.

tribunales chilenos, ya sea por la lectura de decisiones extranjeras o por «estándares interamericanos». Es interesante comparar la experiencia del derecho al olvido presentada en el caso *Mario Costeja* con la experiencia chilena sobre el mismo tema. Para ese acometido, mucho contribuye el libro *Privacidad y protección de datos personales: Jurisprudencia seleccionada y comentada,* en el que Pablo Contreras Vásquez, Michelle Bordachar Benoit y Leonardo Ortiz Mesías (2022: 85) comentan los principales casos de la Corte Suprema de Chile.

En definitiva, la jurisprudencia chilena no es uniforme, pero tiende a no reconocer el derecho al olvido, basándose en diferentes argumentos. Solo en uno de los casos evaluados la Corte Suprema entendió que el derecho al olvido sería aplicable como derecho de cancelación de datos personales por cuestiones concretas. La Ley 19628 (Ley de Protección de Datos Personales) solo prevé el derecho a la cancelación, no a la desindexación. En dicho caso, habiendo transcurrido un determinado lapso de la información obtenida, aunque esta sea veraz, la cancelación sería posible en defensa del honor.[16] Es decir, debido al tiempo recurrido, la información se considera obsoleta o caducada (Muñoz, 2016: 255).

Cabe señalar, por lo tanto, que en el Poder Judicial chileno existe algún tipo de protección del derecho a la privacidad que puede desembocar en el eventual amparo de la protección de datos personales. Un entrevistado de la sociedad civil lo explica bien al mencionar que su entidad comenzó a emprender un litigio estratégico para buscar la consolidación de entendimientos judiciales sobre el tema. Explica que hubo algunas victorias, entre ellas el pago de daños morales debido a una brecha de seguridad de la información. También se muestra escéptico y considera que existen barreras de acceso a la justicia que dificultan la construcción jurisprudencial en Chile del derecho a la privacidad y la protección de datos personales (Veronese y otros, 2023b: 1247-1248). Además, hay posición doctrinaria a favor de que la Ley de Tramitación Electrónica, de 2015, en conjunto con el principio de publicidad, concluye en una cesión forzada de la titularidad de los datos personales o sensibles de las personas que usan el sistema judicial (Bustos, 2018).

Un tema muy actual es el tratamiento de datos personales para lo penal, que fue abordado en detalle por dos entrevistados de la sociedad civil del país. En ese contexto, han hecho mención del deseo de la policía chilena de algún tipo de cooperación con ese fin. Sin embargo, les preocupan los riesgos de abuso que puedan existir (Veronese y otros, 2023b: 1197-1198). Otro entrevistado de la sociedad civil señaló que, durante el debate para modificar la ley chilena de delitos informáticos, la policía presentó solicitudes a favor de aumentar su competencia, con reducción de límites previos y posteriores. Estas solicitudes no se aprobaron, y uno de los principales ar-

16. Sentencia del caso *Graziani contra El Mercurio*, Corte Suprema, rol 22243-2015, 21 de enero de 2016.

gumentos para ello fue la necesidad de restringir esas facultades (Veronese y otros, 2023b: 1199).

Chile es un excelente ejemplo de país en el que se está debatiendo la necesidad de modificar el ordenamiento jurídico a favor de aumentar la protección de los datos personales y la privacidad incluso para integrarse aún más al escenario global. Por ejemplo, Chile aprobó el Marco Legal de Ciberseguridad, posicionando al país como el primero de América Latina y el Caribe que contará con una Agencia Nacional de Ciberseguridad y con un marco regulatorio de vanguardia en esa materia (Bordachar Benoit, 2023). Esa ley es resultado de la implementación del Convenio de Budapest sobre Cibercrimen (Álvarez-Valenzuela y Havia Angulo, 2020).

El caso de Brasil es muy diferente al de Chile. A pesar de la tardía introducción del tema de la protección de datos personales y la privacidad en la agenda política y social, lo que se nota es que este gana cada vez más terreno. El mayor ejemplo fue la promulgación de la Enmienda Constitucional 115/2022 para que el derecho a la protección de datos personales sea autónomo en relación con los derechos de la personalidad. El tema de la protección de datos personales en Brasil fue guiado por estudios académicos, como la tesis pionera de Danilo Doneda (2006). Ese escenario era similar a lo que ocurrió, por ejemplo, en Argentina y Colombia.

El tema de la regulación nacional con un enfoque en Internet aumentó en Brasil alrededor de la década del 2010 debido a varios factores, desde el creciente empleo de aplicaciones de comunicación (como las redes sociales) en los procesos políticos hasta la aprobación del Marco Civil da Internet (Ley 12695/2014), en el que se debatió el tema de la protección de datos personales y se introdujo para una futura agenda política. Esa agenda terminó redundando en 2018 en una legislación brasileña. Es conocido el diagnóstico de que la aprobación de los proyectos de ley que estaban en el Congreso Nacional fueron una respuesta necesaria de integración social y económica de Brasil al paradigma global. Aunque la Ley General de Protección de Datos Personales (Ley 13709/2018) disponga una *vacatio legis* de dos años, eso sirvió como parte de la base legal para la sentencia conjunta de las Acciones Directas de Inconstitucionalidad 6387, 6388, 6389, 6390 y 6393 en 2020. Esa situación no hizo más que reforzarse con la creación de la Agencia Nacional de Protección de Datos (ANPD), como lo diagnostica la producción científica emergente sobre el tema en el país (De Oliveira, 2020: 390; Keller, 2019: 246; Gutiérrez, 2019: 403).

Así, el paradigma brasileño de inserción internacional, desde el punto de vista constitucional, legal e institucional, parece estar centrado en la modernidad jurídica, aunque tardíamente en comparación con varios países de la región, como ya se señaló ampliamente en esta investigación. Hay dos puntos de desarrollo futuro para que esa imagen se vuelva más nítida. El primer paso será la implementación y efectividad de la ANPD en su desempeño regulatorio, ya sea por sí sola o en cooperación con otros órganos y entidades de la Administración Pública Federal. El segundo punto

es la evolución judicial de la cuestión. Según uno de los académicos entrevistados de Brasil, habría esperanzas de que el Poder Judicial se hiciera cargo del tema. Eso habría ocurrido con el derecho del consumidor, y uno de los temas centrales para decir «ahora el tema se ha puesto de moda; adaptémonos todos en la medida de lo posible, porque eso es fundamental» (Veronese y otros, 2023a: 200) sería contar con un gran número de decisiones judiciales en materia de protección de datos personales y privacidad, especialmente con la atribución de responsabilidad civil. En línea con esto, según una entrevistada de la sociedad civil, el tema legal de la responsabilidad civil es clave para que el Poder Judicial asuma más protagonismo en la protección de datos personales. Sin embargo, es pesimista en su diagnóstico, porque no cree que en el corto plazo haya un volumen de decisiones judiciales suficientes sobre el tema (Veronese y otros, 2023a: 200-202).

Anteriormente se señaló que el Poder Judicial argentino fue importante para concretar los reclamos de acceso a la información por medio del *habeas data*, a pesar de la dificultad inicial para aprobar una ley específica que regulara el artículo 43 inciso tercero de la Constitución, luego de su amplia reforma en 1994 (Puccinelli, 2014). Según un entrevistado del Gobierno, la acción judicial en el periodo era esencial (Veronese y otros, 2023b: 1311). La Ley de Protección de Datos Personales de Argentina (Ley 25326/2000) parecía necesaria para corregir las deficiencias e insuficiencias del *habeas data* y el juicio de amparo como medios procesales para proteger derechos relacionados con la información y los datos. El marco legal que se utilizaba tuvo su puesta en vigencia en 1967, pero resultó ser inadecuado, según constata un entrevistado del área académica (Veronese y otros, 2023b: 1281). Esa necesidad era tan evidente que, a pesar del veto al proyecto de ley de 1996, su estructura resultó de utilidad y fue aprovechada posteriormente (Puccinelli, 2004: 45). Además, debido al federalismo argentino, el tema pasó a formar parte de la agenda legislativa de las provincias, hecho que repercutió en el derecho federal (Basterra, 2008b: 26).

Como se indicó anteriormente, factores relacionados con la inserción internacional fueron determinantes para que Argentina aprobara su legislación (Veronese y otros, 2023b: 1411 y 1281). La casuística argentina fue un factor motivador para la inclusión del tema en la agenda pública. Además del famoso caso *Facundo Urteaga* en 1998, en 2014 se llevó a cabo el juicio de la causa *Belén Rodríguez contra Google e Yahoo!*,[17] que se refería a la cuestión de la responsabilidad civil de los proveedores de búsquedas en relación con el contenido indexado, resuelto por la Corte Suprema de la Nación. Los proveedores ganaron el caso y pudieron descartar la responsabilidad objetiva. A menudo se hace referencia a *Belén Rodríguez* como un caso sobre el derecho al olvido, aunque su enfoque se ha centrado en la responsabilidad de los

17. Sentencia del caso *Rodriguez, María Belén c/ Google Inc s/daños y perjuicios*, Corte Suprema de Justicia de la Nación Argentina, rol 522.XLIX, 28 de octubre de 2024, disponible en https://tipg.link/l-M91.

proveedores y la libertad de expresión (Palazzi, 2021: 130). El caso más cercano a la influencia internacional, con foco en el derecho al olvido, es el de *Natalia Denegri*, juzgado en 2022.[18] Una vez más, la Suprema Corte de Justicia de la Nación valoró la libertad de expresión (Veronese y otros, 2023b: 1381).

Casos como estos suelen ser presentados por celebridades que solicitan la desindexación de los motores de búsqueda sobre hechos de su pasado que por alguna razón son motivo de vergüenza. Cabe destacar que ninguno de esos casos ahondó en el uso de imágenes y este solo se trata de manera accesoria en el pleito principal. Por lo tanto, no existe jurisprudencia consolidada sobre los límites al derecho a la imagen en las redes sociales y sobre la responsabilidad de los proveedores en los daños y perjuicios a los titulares de los datos personales.

Otro caso importante fue *Halabi* en 2009, que trató sobre la inconstitucionalidad de la Ley 25873 y su Decreto Reglamentario 1563/2004, que disponía de la capacidad de intervención del poder público en las comunicaciones privadas para recopilar metadatos de telecomunicaciones.[19] Esa interferencia se debió a solicitudes de registros que debían almacenarse indefinidamente. Este caso es reconocido por ser la primera demanda colectiva en llegar a la Corte Suprema de la Nación Argentina. Con base en ese caso, la Corte Suprema calificó la inviolabilidad de las comunicaciones como un derecho fundamental. Argentina está inmersa en el proceso de reforma de su Ley de Protección de Datos Personales, lo que refuerza el impulso existente para mantener el rol protagónico del país en la materia en la región.[20]

Contrario a lo que se observa en la jurisprudencia argentina, en México no se han identificado muchos casos judiciales relevantes en materia de protección de datos personales. De acuerdo con un entrevistado del sector empresarial, eso se debe a que el Poder Judicial mexicano ha sido históricamente ajeno al tema (Veronese y otros, 2023a: 660). Sin embargo, en 2021, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) presentó una demanda constitucional que desató un gran debate nacional en torno al Padrón Nacional de Usuarios de Telefonía Móvil. El padrón pretendía que las empresas de telecomunicaciones recibieran datos biométricos para combatir los actos ilícitos cometidos por las líneas telefónicas, según las respuestas al cuestionario de la encuesta, amablemente respondido por el INAI (Veronese y otros, 2023a: 641). Contó con la participación de varias

18. Sentencia del caso *Denegri, Natalia Ruth c/ Google Inc*, Corte Suprema de Justicia de la Nación Argentina, ID FA22000052, 29 de junio de 2022, disponible en https://tipg.link/l-MG.

19. Sentencia del caso *Halabi, Ernesto c/ P.E.N. – Ley 25.873 – dto. 1563/04 s/amparo Ley 16.986*, Corte Suprema de Justicia de la Nación Argentina 24 de febrero de 2009, disponible en https://tipg.link/loUG.

20. Al respecto, véanse todos los documentos descargables en la página de la Agencia de Acceso a la Información Pública: «Proyecto de Ley de Protección de Datos Personales», *argentina.gob.ar,* disponible en https://tipg.link/l-NQ.

organizaciones de la sociedad civil, como Amicus Curiae, que también contribuyeron a ampliar el debate. El INAI y las entidades de la sociedad civil mantienen una buena relación y el escenario es positivo para la expansión de la agenda de protección de datos personales en el país. Otros casos versaron sobre el estado de salud, los expedientes médicos en instituciones de salud públicas y las fotografías de servidores públicos (Hidalgo Rioja, 2018: 29).

Uruguay es otro país en el que el tema ha cobrado poca repercusión judicial (Veronese y otros, 2023a: 299), a pesar de contar con un sistema administrativo fuerte. Al igual que Argentina, Uruguay fue un país directamente influenciado por el movimiento para aprobar la Directiva 95/46/CE en 1995 por parte de la Unión Europea, que sigue avanzando en el espacio político y administrativo del país. Uruguay también intentó obtener una decisión de adecuación de la Comisión Europea, como evidencia la entrevista a una académica sobre el tema (Veronese y otros, 2023a: 343). Asimismo, según otra entrevistada del área académica, la llegada del Reglamento General de Protección de Datos traerá consigo la necesidad de promover nuevas discusiones, que habrían quedado de lado debido a las prioridades del Gobierno recién electo y la pandemia (Veronese y otros, 2023a: 362). Otra muestra de inserción ha sido la buena relación con el Consejo de Europa, tal y como informan dos entrevistados de la Unidad Reguladora y de Control de Datos Personales de Uruguay (Veronese y otros, 2023a: 374-377).

Finalmente, en el caso de Panamá, el escenario es aún demasiado incipiente para describir la influencia de los organismos internacionales y la jurisprudencia. Sin embargo, es cierto que la legislación y su regulación, como ya se describió en el panorama nacional, se ven influenciados porque el país evoluciona como prestador de servicios internacionalmente.

Al comparar el escenario de los países encuestados, es claro que existe una influencia internacional en la formación de estándares legales, así como en las creencias y acciones sociales relacionadas con la protección de datos personales y la privacidad. Se intentan anclar los significados jurídicos locales con los documentos internacionales (como los tratados) y también es evidente un esfuerzo por observar lo que ocurre en el exterior para interiorizar los significados jurídicos. Ahora bien, el camino para definir la protección de datos personales como derechos constitucionales o fundamentales es diferente. Existen algunas similitudes entre algunos países, como, por ejemplo, una mayor influencia del debate judicial con antecedentes constitucionales (Argentina y Costa Rica) o la predominancia del tema en la agenda administrativa (Colombia). Lo que une a todos los países analizados es el claro intento de organizar sus sistemas jurídicos de acuerdo con un paradigma que consideran parte de la modernidad, directamente relacionado con el futuro social y económico. Para arrojar más luz sobre el debate, la siguiente sección se dedicará a la comparación, centrándose en las especificidades de los países investigados de la región.

Discursos a favor de las especificidades institucionales y culturales (nacionales y locales) de la protección de la privacidad y los datos personales

Los contextos nacionales y locales determinan la construcción del derecho en términos efectivos. Los significados legales y las prácticas sociales diferirán debido a diversos factores sociales, económicos y políticos. ¿Qué hace que la protección de datos personales y la privacidad se gestione socialmente de manera diferente en México y Argentina, por ejemplo? La misma preocupación se aplica a los demás países encuestados. Todas las investigaciones de campo muestran que existe cierto grado de atención en América del Sur y el Caribe respecto a lo que sucede en los países vecinos.

Singularidades nacionales

Una lectura apresurada del panorama de América del Sur y el Caribe podría hacernos creer que la realidad se resumiría a un sencillo intento de copiar modelos extranjeros, en particular el de la Unión Europea o el de Estados Unidos, transmitidos especialmente por medio de intercambios entre entidades y organismos estatales, académicos y la sociedad civil. La investigación muestra que, aunque se les consideren como ejemplos fundamentales, no hay necesariamente una influencia directa, pues hay una adaptación y transformación de ellos según los contextos nacionales y locales.

Es posible sintetizar algunas peculiaridades. Empecemos por Chile, país que es parte de la Organización para la Cooperación y el Desarrollo Económico, y está influenciado por el eje económico y social de Asia y el Pacífico por medio de la APEC y el Digital Economy Partnership Agreement (Veronese y otros, 2023b: 1161). Esto lo coloca en un rol especial, desde el que puede lidiar con diversos estándares y mercados, con el potencial de crear un tipo específico de protección de datos personales. Chile tiene la ley más antigua y está encajonado entre la tradición de la Unión Europea y la de Estados Unidos, así como la de Asia y el Pacífico. Ese dilema sobre direcciones y modelos se hace evidente al leerse la crítica que hace una entrevistada a que Estados Unidos no cuente con un marco legal claro sobre el tema (Veronese y otros, 2023b: 1235). Ese discurso demuestra cómo Chile se encuentra en medio de un momento interesante en la materia, con varias posibilidades abiertas para complementar su modelo de protección de datos personales y privacidad. Al respecto, el presidente Joe Biden publicó en 2023 un artículo de opinión en el *Washington Post,* en el que instó al Congreso de Estados Unidos a discutir y aprobar una ley federal para la protección de la privacidad en Internet.[21]

21. Joe Biden, «Republicans and Democrats, unite against Big Tech abuses: Congress can find common ground on the protection of privacy, competition, and American children», *The Wall Street Journal*, 11 de enero de 2023, disponible en https://tipg.link/lofs.

México es otro país con singularidades. La primera es su estructura federada en lo que atañe al sistema de protección de datos personales, en el que el INAI actúa como órgano de revisión de las decisiones locales. Su dualidad de leyes también es peculiar. Desde 2010, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares es aplicable al sector privado, pero para el área pública había varias leyes estatales. Ese marco solo se armonizó con la creación de una ley federal en 2017: la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Ese proceso también está conectado a la reorganización de la autoridad de protección de datos (el INAI), con la ampliación de su competencia a todo el país, en cooperación administrativa con las autoridades estatales.

Según una entrevistada del sector empresarial, la dualidad de las leyes puede explicarse por el temor del sector privado a que una sola legislación pueda ser una carga demasiado pesada para la industria y las empresas. No obstante, él también manifiesta disconformidad con la solución, ya que —según explica— no está claro para los ciudadanos y empresarios, en determinadas situaciones, qué ley estatal es aplicable, ya que existen treinta y dos leyes estatales y distritales, además de la ley federal (Veronese y otros, 2023a: 653). Según algunos estudiosos, el ideal sería, quizás, promover la separación entre la protección de los datos personales y la privacidad del acceso a la información pública (Jijena, 2013; Matus, 2013). Sin embargo, algunos de los entrevistados, miembros del INAI, discrepan, pues consideran necesario equilibrar la protección de datos personales con el acceso a la información pública (Veronese y otros, 2023a: 645-646).

Aunque la protección de datos personales de los ciudadanos deba ser un límite al derecho de acceso a la información, es necesario considerar el contexto de cada caso y la naturaleza del dato personal involucrado (Jijena, 2013: 65). Por ejemplo, dentro de la judicatura, hay varios casos judiciales en los que se debe tener un cuidado especial a la hora de respetar el principio de publicidad, porque tratan datos privados sensibles, como procedimientos de cambio de sexo, datos médicos sanitarios y cuestiones laborales (Guerrero Guerrero, 2020: 50). De acuerdo con una entrevistada del sector empresarial, el tema del acceso a la información pública tendría culturalmente un mayor prestigio en México que la protección de datos personales, por ejemplo (Veronese y otros, 2023a: 669).

Semejante conclusión nos da una representante de la sociedad civil, quien subraya que el sólido y reconocido desempeño del INAI termina por empañar su desempeño en materia de protección de datos personales. Ese hecho incluso tendría repercusiones en las autoridades estatales y en la capital federal (Veronese y otros, 2023a: 680-682). Finalmente, para otra entrevistada del área de negocios, eso se reflejaría en la asignación de recursos para proteger datos personales, que se perjudicaría en comparación con la defensa del acceso a la información pública (Veronese y otros, 2023a: 698).

Otra peculiaridad jurídica y formal de México es que el tema evolucionó a partir del derecho de acceso a la información (Parra Noriega, 2011: 155). Si bien ese derecho fue constitucionalizado en 1977, la Constitución del país no contempló el *habeas data* como medio procesal (Arroyo Kalis, 2017: 65). Eso significaba que el medio procesal a utilizar ante el Poder Judicial era el juicio de amparo, que guarda, en cierta medida, similitud al *mandado de segurança* brasileño (Veronese y otros, 2023a: 661). Es interesante también el caso de Argentina, en el que la creación de la Ley de Protección de Datos Personales fue acompañada por la formalización del *habeas data*.

En cuestión de participación social, analizamos el caso de Argentina, Brasil y México. Argentina cuenta con mecanismos de participación social en el seno de la Agencia de Acceso a la Información Pública. Así, es posible contrastar el caso argentino con el brasileño. En este último, existe una gran capacidad de articulación de las organizaciones de la sociedad civil en torno a esos temas, que es expresada por la Coalición Derechos en la Red (Coalizão Direitos na Rede), en contraste con otros países con grandes extensiones territoriales como Argentina (Veronese y otros, 2023b: 1421) y México (Veronese y otros, 2023a: 768). En el caso argentino, la designación de los directores de la autoridad de protección de datos es realizada por el Poder Ejecutivo, con la aprobación del Senado (Veronese y otros, 2023b: 1345-1346). La sociedad civil ya ha logrado presionar al Gobierno para que no dictamine en determinado sentido, lo que demuestra la existencia de presión social, a pesar de la falta de una coalición formal (Veronese y otros, 2023b: 1413). En el caso de México, las organizaciones de la sociedad civil llevan a cabo su articulación a nivel internacional efectivo, conformando coaliciones como la Global Encryption Coalition (2022) y AlSur.[22]

Uruguay y Argentina tienen la singularidad de dedicar disposiciones legales específicas en sus leyes al tratamiento de datos personales en materia de publicidad; ni el Reglamento General de Protección de Datos presenta ese rasgo ni lo hacen los estándares de la Red Iberoamericana de Protección de Datos (RIPD). Esas normas sobre el tratamiento de datos con fines publicitarios reconocen el derecho de acceso y son compatibles con los principios generales de la legislación (Durán Martínez, 2012: 71). Un entrevistado escéptico afirma que la ley uruguaya sería una copia de la ley argentina (Veronese y otros, 2023a: 314). Otro ejemplo de la similitud entre Uruguay y Argentina es que esos países miran a la Unión Europea como un modelo esencial, lo que explica la similitud de las leyes, según declaran entrevistadas académicas (Veronese y otros, 2023a: 321 y 400). La similitud también se expresa, según explica una entrevista a la autoridad de protección de datos (la Unidad Reguladora y de Control de Datos Personales), en que Uruguay ha sido el segundo país de la región en recibir

22. Para más información sobre las coaliciones, véase «About Global Encryption Coalition», *globalencryption.org*, disponible en https://tipg.link/l8H_, y «Qué hacemos», *alsur.lat*, disponible en https://tipg.link/l8I6.

una decisión de adecuación de la Comisión Europea, después de Argentina (Veronese y otros, 2023a: 374).

Esa influencia indirecta de la Unión Europea también se dio en Panamá y Brasil, aunque con resultados institucionales diferentes. Panamá siguió el modelo mexicano de sumar la protección de datos personales al acceso a la información pública y la lucha contra la corrupción, mientras que Brasil creó una autoridad autónoma de protección de datos personales. El tema del acceso a la información pública y la lucha contra la corrupción se ha integrado más en la Contraloría General de la Unión, que tiene el estatus de ministerio en Brasil.

La singularidad de Costa Rica es que la Sala Constitucional ha tenido un papel histórico, desde antes del 2000, al importar la «autodeterminación informativa» y ocuparse de las nuevas tecnologías de la información y la comunicación. Ha dado lugar a una interesante jurisprudencia que, incluso antes de la llegada de la Ley 8968/2011 de protección de la persona frente al tratamiento de sus datos personales, regulaba la protección de datos personales. Hasta el día de hoy, el Poder Judicial tiene un papel evidente en el país, lo que despierta críticas. Un ejemplo es la sentencia de la Sala Constitucional, que excluyó la condición de estar vacunado de la categoría de datos personales sensibles (Veronese y otros, 2023b: 858).

En el caso de Perú, es interesante destacar la regulación cooperativa entre la autoridad de protección de datos y el Instituto Nacional de Defensa de la Competencia y la Protección de la Propiedad Intelectual. Esa entidad administrativa tiene competencia para actuar en el ámbito del derecho del consumidor, lo que trae la necesidad de aunar esfuerzos en el ámbito de la protección de datos personales (Veronese y otros, 2023a: 535).

Colombia presenta una autoridad de protección de datos que es peculiar, ya que no se combina con el acceso a la información pública (algo que sucede en Argentina, México y Panamá, por ejemplo), sino que se inserta dentro de un organismo muy fortalecido en el contexto nacional, vinculado al Ministerio de Economía, que es la Superintendencia de Industria y Comercio. Esa autoridad tiene amplias atribuciones en el ámbito de la competencia y la protección del consumidor. Está gestionada por un oficial designado y la protección de los datos personales es responsabilidad de una subcomisión. Esta última tiene una historia reciente de mucha actividad, incluso con gran impacto mediático, incluidos otros países. Un rasgo llamativo de Colombia es el aumento significativo en el número de quejas y órdenes emitidas (Veronese y otros, 2023b: 1017).

Otra singularidad brasileña, además de la participación de la sociedad civil organizada, se encuentra en la rápida aprobación de la Ley 13709/2018 y en el compromiso de la comunidad jurídica en el tema. El proceso de aprobación fue tan rápido que terminó generando la necesidad de cambios rápidos para asegurar la construcción de la ANPD (Veronese y otros, 2023a: 174). En el proceso de modificación de la ley hubo

otros cambios, como la imposición de un veto a la disposición (párrafo 3 del artículo 20 de la Ley General de Protección de Datos de Brasil) que disponía la revisión humana de las decisiones exclusivamente automatizadas. De acuerdo con una entrevistada vinculada a las empresas, la industria hizo presión al estimar que tal pronóstico retrasaría el desarrollo tecnológico brasileño (Veronese y otros, 2023a: 122).

En otro aspecto del tema, un entrevistado de la autoridad de protección de datos indicó que esa imposición determinaría un aumento de costes para las entidades de crédito, obligadas a crear muchos equipos para llevar a cabo esa tarea, aunque él y la ANPD son conscientes de los riesgos de los sistemas automatizados (Veronese y otros, 2023a: 48). Una académica entrevistada menciona que, a pesar del veto, el tema aún no está completamente definido debido a la aplicabilidad de otros derechos y principios fundamentales (como la transparencia, la contradicción y el debido proceso legal) a decisiones automatizadas que restringen derechos (Veronese y otros, 2023a: 206).

Es difícil crear una clasificación única entre los distintos países investigados. Existen varias vías nacionales para incorporar la protección de datos personales y la privacidad, ya sea en los sistemas jurídicos, en las estructuras institucionales o en los medios de defensa (judiciales o administrativos). Esa comparación deja claro que las visiones simplistas de América Latina pueden llevar a interpretaciones equivocadas. Parece claro, igualmente, que el concepto de protección de datos personales y privacidad se está construyendo en varios países de la región, aun cuando presenta diferencias institucionales interesantes relacionadas con los contextos culturales específicos. Incluso si se intenta importar el concepto de protección de datos personales de la Unión Europea como un derecho fundamental, los medios para su implementación serán diversos. En la siguiente subsección, se visualizará cómo el tema del tratamiento de los diversos grupos sociales, existentes en el seno de los diversos países, apareció en las entrevistas y documentos de investigación.

Singularidades nacionales de grupos sociales específicos

No es de extrañar que el tema de la protección de los menores legales surja en varias entrevistas y esté en la agenda de varios países. Ese tema es, de hecho, global, pero los medios para lograr la protección de niños, niñas y adolescentes varían en los diferentes países. En el caso de Costa Rica, ya se abordó el caso *Faro*, referido a los exámenes que el Gobierno trató de aplicar a los niños y que ha llevado a una gran agitación política y legal. En Perú, es interesante resaltar que en una entrevista la autoridad de protección de datos comentó sobre el tema, relacionándolo con la RIPD —organización activa que no es un organismo internacional— y sus estándares como base para toda la región (Veronese y otros, 2023a: 538). En Uruguay también se mencionó la preocupación por niños, niñas y adolescentes como un problema relevante por dos

entrevistados del área académica y por un miembro de la autoridad de protección de datos (Veronese y otros, 2023a: 306, 355 y 386).

En el caso de Colombia, hubo una polémica respecto a los sistemas de control digital, los datos de salud y, por ende, los datos sensibles de los ciudadanos. La aplicación nacional creada para dicho control, que generaba un código QR para permitir el acceso a determinados espacios (Veronese y otros, 2023b: 1033), ha enfrentado varias controversias, como manifestó un miembro de la autoridad de protección de datos (Veronese y otros, 2023b: 1016). Según explica un entrevistado de la sociedad civil, había dificultad para garantizar el uso adecuado de los datos personales recopilados y procesados por la aplicación (Veronese y otros, 2023b: 1109). Para ellos, esa acción se vio agravada, pues la posibilidad de que la SIC sancionara cualquier desviación sería casi nula, ya que no tendría la competencia ni autonomía para investigar y punir a los agentes públicos (Veronese y otros, 2023b: 1056).

El tema del género y la violencia contra la mujer es igualmente de interés de Costa Rica y Panamá. En el caso de Costa Rica, se indicó la cooperación para que un centro de investigación funcione bien, con la colaboración de la Agencia Española de Protección de Datos, así como de Facebook y otras plataformas digitales. El objetivo, según una entrevistada del área de negocios, es crear una forma accesible de tratar esos casos en canales especializados, en cooperación y con la capacitación de agencias y entidades gubernamentales. La misma entrevistada se refiere al proyecto Eurosocial y a la Organización de Estados Americanos como elementos de apoyo al esfuerzo (Veronese y otros, 2023b: 901).

En el caso de Panamá, se visibilizó la necesidad de empoderamiento de las mujeres, citando la cooperación de la autoridad de protección de datos —la Autoridad Nacional de Transparencia y Acceso a la Información (Antai)— con el Instituto Nacional de las Mujeres para crear canales de protección contra la violencia de género por medio de aplicaciones, entre otras cuestiones. Esas acciones culminaron en la creación de la *Guía para el tratamiento de datos para mujeres víctimas de violencia* y en acciones de colaboración con la Unesco. El tema lo mencionaron expresamente los entrevistados de Antai al señalar la necesidad de atender a grupos vulnerables, como inmigrantes, pueblos indígenas, mujeres, niños, niñas, adolescentes y personas con VIH (Veronese y otros, 2023b: 1524).

En el caso de México, cabe destacar que el INAI realizó una encuesta nacional en 2019 con apoyo del Instituto Nacional de Estadística y Geografía (INEGI) de percepción social en materia de protección de datos.[23] En la última edición del estudio, realizada en 2018, surgió algo que la literatura denomina la «paradoja de la privacidad». Se puede resumir esta paradoja como la creencia por parte de las personas de que hay un empleo menoscabado de sus datos personales y, a pesar de ello, no se adop-

23. Se trata de la Encuesta Nacional de Percepción Ciudadana, disponible en https://tipg.link/l-Nw.

tan medidas para mitigarlo. En esa encuesta, el 50% de la población dijo desconocer la existencia del INAI y el 93% admitió que nunca había presentado ninguna queja sobre el uso indebido de sus datos personales. Ese fenómeno y los datos de la investigación parecen ser un problema grave, en opinión de un entrevistado académico, ya que afectarían aún más a los niños y adolescentes (Veronese y otros, 2023a: 688). La paradoja de la privacidad también apareció en entrevistas con dos académicas de Argentina (Veronese y otros, 2023b: 1284 y 1300). Una tercera entrevistada académica relacionó el problema con la vulnerabilidad de los niños, niñas y adolescentes.

Finalmente, al analizar el caso de Brasil, las entrevistas trajeron el tema racial al debate. Uno de los entrevistados mostró su preocupación por el tema del reconocimiento facial y las cuestiones raciales. También criticó la ausencia de personas negras en el Consejo Nacional de Protección de Datos y en la conducción de la ANPD (Veronese y otros, 2023a: 194). La cuestión racial es un problema estructural en Latinoamérica, caracterizado por el daltonismo racial, en el que las personas suelen creer que las desigualdades y la discriminación racial han sido superadas debido al mestizaje ocurrido en esos países. Eso se convierte en un desafío a superar que se ve acentuado por el paradigma de la discriminación algorítmica, en el que las tecnologías emergentes que procesan datos personales de forma masiva, como la inteligencia artificial, terminan acentuando aspectos discriminatorios inculcados en las sociedades de esos países y reforzando el racismo estructural (Muñoz Gutiérrez, 2021: 292).

El tema de los grupos sociales específicos terminó extendiéndose más a los grupos expuestos o vulnerables. No había forma de evaluar hasta qué punto los aparatos judiciales o administrativos de protección de datos personales y la privacidad son eficaces para tratar con esos grupos sociales específicos ni si ellos perciben el concepto de datos personales de manera diferente a la de la población. Hay pistas sobre las posibles culturas sociales y las demandas legales específicas sobre el tema, según entrevistados académicos, miembros de gobiernos y autoridades de protección de datos, y representantes de la sociedad civil.

Dificultades locales para acceder y comprender los derechos de los titulares de los datos personales y la privacidad en los distintos países

Ese tema se puede resumir en tres grandes cuestiones que sin duda afectan a las poblaciones de los distintos países latinoamericanos: i) la brecha digital; ii) las barreras al acceso a la justicia y al sistema de protección administrativa; y iii) las dificultades para crear conciencia. Esos tres factores son bastante preocupantes. La efectividad del derecho a la protección de datos personales y a la privacidad depende de la participación social y de un acuerdo entre el Estado, la sociedad civil y las empresas. Por lo tanto, ha sido muy relevante recopilar entrevistas y analizar documentos de diversas fuentes para identificar esos dilemas en los países encuestados.

Es posible comenzar esa descripción y análisis con el caso de Perú, del cual se desprenden los dichos de una entrevistada de la sociedad civil que considera que la población del país no manifiesta un grado elevado de preocupación por la protección de sus datos personales y su privacidad. Su discurso expresa un sentimiento que puede identificarse en varios países de la región y, quizás, también en el resto mundo. Al informar sobre temas como la videovigilancia y el reconocimiento facial, esta dice que buena parte de la población reacciona así: «Pueden monitorearme y recopilar mis datos personales; no me importa, no debo nada» (Veronese y otros, 2023a: 449).

Al revisar la historia normativa del tema, una entrevistada del sector empresarial peruano menciona que la ley local es de 2011 y su regulación fue puesta en vigencia en 2015. Por lo tanto, esta considera, con bastante optimismo, que se necesitarán diez años para que el tema se generalice. El tema ha ganado terreno en los últimos años y, aunque no puede considerarse que exista una cultura de protección de datos personales en el país, esa realidad va en camino (Veronese y otros, 2023a: 508). La expectativa es que el sistema jurídico peruano sea capaz, poco a poco, de superar el modelo de gestión de datos para adoptar un esquema de responsabilidad proactiva en similitud a otros modelos normativos actuales, siendo así capaz de contemporizarse con el fenómeno del Internet, el *big data*, las redes sociales y la inteligencia artificial, entre otras nuevas formas de tratar datos personales (Zegarra Valdivia, 2019: 205).

En Costa Rica también se mencionó la necesidad de acciones sociales, individuales y colectivas. En ese sentido, según una entrevistada de la sociedad civil, la proactividad de la ciudadanía es muy importante y es fundamental conocer esa «cultura popular en la ciudadanía», algo que se puede interpretar como la mayor rutinización del tema. Aquí, existiría una mayor protección liderada por las acciones de los ciudadanos, basadas en su concienciación, así como buenas respuestas por parte del Estado y las empresas (Veronese y otros, 2023b: 836). La Agencia de Protección de Datos de los Habitantes es la autoridad de protección de datos de Costa Rica. La entrevistada, empleada de la institución, también enfatiza la necesidad de una «educación en bases de datos» para la población general (Veronese y otros, 2023b: 952).

El caso de Chile también es interesante. Una entrevistada del ámbito académico explica que el Consejo para la Transparencia elabora anualmente una encuesta nacional sobre la preocupación social por los datos personales. Según esta, la mayoría de los ciudadanos habrían demostrado en sus respuestas que estaban realmente preocupados. Sin embargo, considera que la práctica social sería diversa, en términos generales. El acceso al número de identificación ciudadana en Chile (rol único tributario o RUT) sería facilitado por todos para obtener rebajas en farmacias, por ejemplo, sin que ello les moleste en absoluto. Es este un ejemplo de la «paradoja de la privacidad» mencionada anteriormente.

Durante la pandemia hubo un hecho digno de nota, pues un grupo de ciudadanos habría comenzado, por su cuenta, a manifestarse —ofensivamente, incluso— contra

la solicitud de sus datos personales por parte de las autoridades a la hora de retirar dinero de los fondos de pensión como ayuda financiera. Ese hecho se reportó en los medios locales[24] y el video aún también disponible en YouTube.[25] El caso sería curioso, ya que existiría una base legal para esa práctica y nunca habría habido ninguna manifestación pública a favor de la protección de datos personales en Chile (Veronese y otros, 2023b: 1228-1229). Es cierto que la sociedad civil chilena cuenta con organizaciones efectivas, como Derechos Digitales y Fundación Datos Protegidos, entre otras, pero una acción de ese tipo, de confrontación y en la calle, fue algo inédito.

En este sentido, una entrevistada del Gobierno chileno explicó que la encuesta anual sobre el tema demuestra la creciente preocupación y señala la elevación de la conciencia de la población sobre el tema de la protección de datos personales. Señaló que habría una mayor preocupación por los anuncios, por ejemplo. Confirmó también que hubo resistencia a entregar el RUT, pero indicó que, cuando hicieron una pregunta sobre datos de salud en la encuesta realizada durante la pandemia, hubo mayor disposición a proporcionarlos (Veronese y otros, 2023b: 1166).

El informe de la ANPD en Brasil sobre el tema de la concientización fue similar al de Panamá. Había indicios de trabajo por realizar y de que la autoridad estaba construyendo convenios institucionales con otras instituciones nacionales e internacionales. En esa línea, una entrevistada subrayó el interés de la ANPD en que el Gobierno brasileño se adhiera al Convenio 108 (Veronese y otros, 2023a: 35). Este tratado del Consejo de Europa es uno de los documentos internacionales más importantes y antiguos sobre protección de datos personales, y se actualizó en 2018.

En Panamá, por su parte, la Antai está realizando campañas y eventos para difundir el tema (Veronese y otros, 2023b: 1503), pese a las críticas de la sociedad civil (Veronese y otros, 2023b: 1470-1471). La entrevistada académica considera que el tema es nuevo y, por lo tanto, se está gestionando en la medida de las posibilidades (Veronese y otros, 2023b: 1446).

En Uruguay, las entrevistas también señalan el problema de la dificultad de conocimiento de los derechos por parte de los ciudadanos como el mayor obstáculo. Una entrevistada académica considera que este es un tema complejo y, por lo tanto, difícil de asimilar por la sociedad (Veronese y otros, 2023a: 352). Esa entrevistada explica el dilema en términos muy lógicos: la población conocería sus derechos y estaría al tanto de los usos indebidos y de los problemas de seguridad de la información, aunque no haya consciencia de los medios que deben movilizarse para proporcionar protección. Ese diagnóstico no es negativo; más bien, en opinión de esa entrevistada,

24. Cristian Neira, «"¿Por qué necesita conocer el RUT?": Briones hace polémica solicitud de datos de quienes retiraron el primer 10%», *El Desconcierto*, disponible en https://tipg.link/l1rF.

25. Véase Teletrece, «Ministro Briones es increpado en la calle», *YouTube.com*, 5 de noviembre de 2020, disponible en https://tipg.link/l1rR.

se debe seguir avanzando (Veronese y otros, 2023a: 352 y 409-410). Ese relato, convergente y positivo, puede resumirse en el fragmento del discurso de otro académico entrevistado, quien reitera que el tema de la protección de datos personales y la privacidad ha avanzado en Uruguay. Esto habría repercutido en una mayor conciencia social, por lo que las empresas estarían considerando esa protección —y el cumplimiento de la legislación— como un valor añadido en sus actividades económicas (Veronese y otros, 2023a: 403).

El encuestado de la autoridad de protección de datos de Uruguay tiene el mismo entendimiento que los encuestados académicos. Explicó que la Unidad Reguladora y de Control de Datos Personales realiza encuestas nacionales anualmente. Los resultados demostrarían efectos positivos, basados en campañas de sensibilización y comunicación sobre la protección de datos personales y la seguridad de la información (Veronese y otros, 2023a: 386). Otra académica entrevistada fue bastante explícita: queda mucho por hacer antes de que podamos hablar de una cultura efectiva de protección de datos personales (Veronese y otros, 2023a: 320).

En Argentina, una académica entrevistada considera que el tema no estaría en el foco general de la población, ya que esta estaría más preocupada de la satisfacción de otras necesidades, especialmente de carácter económico (Veronese y otros, 2023b: 1373). Sin embargo, según otro entrevistado de la sociedad civil, habría una división geográfica y social que explicaría el dilema, de modo que el tema estaría más extendido en las ciudades que en las zonas rurales (Veronese y otros, 2023b: 1419). Una situación similar ocurre en el caso de México, en el que una entrevistada de la sociedad civil indicó la necesidad de viajar a la capital del país, es decir, a la sede del INAI, para hacer valer derechos relacionados con la protección de datos personales (Veronese y otros, 2023a: 760-761), lo que agrega una dificultad extra.

La literatura colombiana diagnostica el dilema de la brecha digital y es un buen punto de partida para esa pregunta. Según un libro reciente publicado sobre el tema, casi el 60% de la población más pobre no utiliza internet en su vida cotidiana, en contraste con cerca del 80% de uso diario de la población más rica (Saavedra Rionda y otros, 2021: 70). Las consecuencias son múltiples, entre ellas la dificultad para acceder a oportunidades y para disfrutar de los servicios públicos.

En Colombia, la autoridad de protección de datos también se pronunció sobre el tema general de la protección de datos, pero centrándose en el problema de la interoperabilidad de los sistemas y su uso por parte de otras entidades estatales. Al respecto, demuestra que la SIC puede emitir órdenes a otras entidades estatales sobre el uso de los datos de los ciudadanos, pero su competencia no le posibilita aplicar sanciones, dado que el ordenamiento jurídico colombiano asigna esa función al Ministerio Público (Veronese y otros, 2023b: 1093). Ahora bien, esa situación jurídica no se convirtió en pasividad por parte de la autoridad. La entrevista en SIC contó con dos participantes de la organización. Un entrevistado de la SIC señala que se emitió

un expediente a otros órganos y entidades del Estado para explicar que los datos personales de los ciudadanos podrían utilizarse en políticas públicas si se observaban los principios legales, que incluían seguridad, transparencia, finalidad y confidencialidad. La persona entrevistada incluso hizo una pregunta: «¿Cómo sería posible crear una política pública nacional efectiva sin interoperabilidad?» (Veronese y otros, 2023b: 1011). De hecho, se trata de un tema recurrente en el debate sobre la protección de datos personales y la privacidad. Las leyes de protección de datos personales no pretenden prohibir el uso de datos personales, sino determinar su uso responsable y controlado.

Otro reflejo de la problemática geográfica y social quedaría claro en la entrevista a un representante de un gobierno estatal mexicano, en ese caso de Jalisco. Este señala que su estado sería uno de los más poblados y que, para hacer cumplir la Ley Contra los Particulares, sería imperativo acudir a la capital. Esa problemática se reflejaría en un menor grado de adecuación de las empresas fuera del capital, además de explicar una menor concienciación de la población en esas zonas (Veronese y otros, 2023a: 742). Cabe destacar que esos relatos sobre la dicotomía entre el medio rural y urbano verificados en países federales como México y Argentina también pueden repetirse en Brasil.

La próxima sección está dedicada a un tema muy relevante para la investigación: las influencias mutuas entre los distintos países latinoamericanos y si eso puede dar lugar a la construcción de una cultura regional de protección de datos personales.

Las influencias de los países latinoamericanos sobre la región: ¿Embrión de una cultura jurídica regional sobre protección de datos personales?

Habría que hacer una advertencia epistemológica. Al equipo de investigación le gustaría ver muchas respuestas que señalasen la existencia de un fuerte tráfico de intercambios culturales entre países, ya sea académico, empresarial o de cooperación estatal. Esa expectativa no indujo un sesgo en el sentido de distorsionar las informaciones obtenidas. Esos intercambios existen y su ejemplo más evidente es la existencia de la RIPD. La respuesta a esa encuesta está menos orientada hacia una interacción continua y más a un proceso de recepción nacional y local de parámetros, prácticas y creencias que se han desarrollado en otros países, como los Estados miembros de la Unión Europea, los miembros de APEC, los estándares de la Organización para la Cooperación y el Desarrollo Económico e incluso acciones de empresas con alcance global, como las grandes plataformas.

Esos instrumentos y otros similares tienen una importante coherencia que ha contribuido a configurar normas de protección de datos que han llegado a ser reconocidas por varios países latinoamericanos, como Chile (Arrieta Cortés, 2009: 15). Esa búsqueda de convergencia y armonización de conceptos, principios y normas

de protección de datos se ha convertido incluso en objeto de atención de la RIPD, que en 2017 publicó los Estándares de Protección de Datos Personales.[26] Dichos estándares recogen las mejores prácticas nacionales e internacionales en la materia y proponen una serie de instrumentos flexibles para facilitar su adopción entre los Estados iberoamericanos, sin menoscabo de los derechos nacionales. Asimismo, busca garantizar un nivel adecuado de protección de los datos personales en la región, con el objetivo de no establecer barreras a su libre circulación en los Estados iberoamericanos y, en consecuencia, favorecer las actividades comerciales entre la región, así como con otras regiones económicas (Puccinelli, 2020: 35).

En Perú, según un entrevistado de la sociedad civil, abogado, a menudo habría copias de otros países de la región, aunque eso se realizaría en paralelo con el modelo de la Unión Europea. La explicación para copiar modelos de la región sería la similitud socioeconómica con sus vecinos (Brasil, Colombia, Argentina y Chile están directamente listados). En el caso del empleo de modelos europeos, el entrevistado manifiesta cierto temor, ya que considera que la realidad al otro lado del Atlántico sería diferente (Veronese y otros, 2023a: 443). El discurso de la entrevistada hace referencia fuertemente a los modelos de ley y normas. Una entrevistada del área académica fue muy clara al enunciar la influencia de las políticas públicas colombianas en el Perú, incluyendo la enumeración de diferentes temas, como la propiedad intelectual y la gobernanza de Internet (Veronese y otros, 2023a: 580).

Asimismo, la entrevista con una representante de la sociedad civil fue muy esclarecedora. Esta se refiere también a Colombia, como ejemplo, y luego a Chile y Argentina, en términos generales. Cuando se trata de la regulación de la protección de datos personales, señala que Colombia ha sido un ejemplo por seguir, más que Argentina. Considera que Chile se ha quedado rezagado en el tema y que Brasil ha aprobado una legislación interesante, ya que no es una mera copia del Reglamento General de Protección de Datos de la Unión Europea. Sin embargo, se queja de que algunos sectores empresariales y estatales se centrarían solo en Colombia y Brasil, ignorando las experiencias innovadoras que están en curso en Paraguay y Ecuador (Veronese y otros, 2023a: 466).

En el relato de una entrevistada de la sociedad civil costarricense aparece la misma dicotomía. México y Perú son nombrados, pero también se plantea la necesidad de mirar a los vecinos más cercanos (Veronese y otros, 2023b: 835). Una entrevistada del sector empresarial costarricense reconoció la necesidad de fortalecer la RIPD, así como de internalizar los estándares emitidos por ella en la legislación de los distintos países. Su respuesta contiene un poco de especulación sobre el modelo uruguayo, considerándolo antiguo (y por lo tanto más establecido) y proveniente de un país con similitudes en términos de territorio y población. Es interesante notar que desde

26. El texto completo de estos estándares puede revisarse en https://tipg.link/lAGM.

Costa Rica, en la entrevista a la Agencia de Protección de Datos de los Habitantes, se señala que existe un marco efectivo de cooperación con México y una estrecha relación con Panamá, incluyendo un marcado optimismo sobre la nueva ley que allí se aprobó. De esta forma, la noción de escenario centroamericano es evidente (Veronese y otros, 2023b: 950-951).

La imagen de esa región del continente se refuerza en entrevistas con la sociedad civil panameña en las que se menciona directamente a los países de la región, incluyendo detalles de avances y problemáticas (Veronese y otros, 2023b: 1489-1493). También se señala la estrecha relación entre Panamá y Costa Rica en el ámbito del intercambio de experiencias en asuntos de Estado. La entrevista con la Antai de Panamá también puso de relieve esa inquietud por conectar su trabajo con Costa Rica y otros vecinos. Sin embargo, se recalcó la dualidad del enfoque, en tanto se complementa con la observación de los procesos de la Unión Europea (Veronese y otros, 2023b: 1528). Además, la académica entrevistada utilizó el argumento de la relación económica del país con los Estados miembros de la Unión Europea al informarlo en un evento público dirigido a empresas del sector financiero (Veronese y otros, 2023b: 1442).

En el caso de Colombia, es bastante evidente que Argentina y Uruguay son referencias al tener experiencia en el tema, según indica una entrevistada del área académica. Es bien sabido que ambos países cuentan con decisiones de adecuación emitidas por la Comisión Europea. Esa misma entrevistada de Colombia refuerza que el tema ha avanzado en Perú, pero más lentamente de lo que le hubiera gustado (Veronese y otros, 2023b: 1130). Una representante de la sociedad civil reitera la dicotomía entre observar a los vecinos y tener contacto con la experiencia de la Unión Europea, ante lo que señala la importancia de la RIPD. Para esta, Brasil, a pesar de ser un recién llegado al tema, ha generado un impacto en la región al haber creado una autoridad específica con pretensión de autonomía (Veronese y otros, 2023b: 1142).

Es interesante, porque esa entrevistada de la sociedad civil también explica la razón del protagonismo de Colombia en la región. Parte de la respuesta estaría en las investigaciones abiertas por la SIC sobre posibles violaciones masivas a los derechos de protección de datos personales de los colombianos frente a grandes aplicaciones como Facebook o Zoom, entre otras. Eso se vería facilitado por la legislación del país, que sería tecnológicamente neutra y bien gestionada en tales casos. La SIC no es una agencia dedicada exclusivamente a la protección de datos personales, su ámbito de actuación abarca otras competencias, vinculadas a la regulación industrial y comercial, y al derecho de competencia, en un modelo similar a la Comisión Federal de Comercio de Estados Unidos. La entrevista concluyó con el comentario de que sería importante que en el futuro se realizaran investigaciones paralelas, con la combinación cooperativa de varias autoridades, y que la RIPD podría desempeñar un rol en el sentido de facilitar ese proceso (Veronese y otros, 2023b: 1099).

En Chile se mencionaron poco los factores externos y la posible cooperación. Lo más destacado de la entrevista con una representante de la sociedad civil fue APEC, así como la Unión Europea y la Organización para la Cooperación y el Desarrollo Económico (Veronese y otros, 2023b: 1193). De hecho, la experiencia en la resolución de la tensión entre la protección de datos personales y el derecho de acceso a la información pública parece ser un tema que los países latinoamericanos han estado enfrentando. Como reitera un entrevistado miembro del Gobierno chileno, la experiencia de la Unión Europea ha sido recibida de manera específica y singular en los diversos países latinoamericanos (Veronese y otros, 2023b: 1177).

El aislamiento aparece en el caso brasileño. La ANPD es una entidad reciente. Al entrevistar a un representante de la entidad queda claro que, en un primer momento, no hubo una mirada efectiva a las experiencias de otros países latinoamericanos. La atención se centró en los debates en la Unión Europea. Tampoco hizo referencia a la RIPD ni a ningún otro país de la región (Veronese y otros, 2023a: 85). Dicho eso, se sabe que la ANPD es miembro de RIPD desde 2021[27] y que participa en reuniones de la red, como la que tuvo lugar en abril de 2024.[28] En esas reuniones se discutió la organización de acciones coordinadas para abordar procesamiento de datos y experiencias personales de tecnologías emergentes como ChatGPT y Worldcoin.

El caso de Argentina es muy diferente. Es el país con una autoridad de protección de datos y una legislación más antigua, además de obtener una decisión de adecuación de la Comisión Europea. En entrevistas con una representante de la sociedad civil y una representante del Gobierno, ambos plantean el rol de Argentina en la conformación de la RIPD, así como el impulso que el país ha intentado emprender en la materia en el marco del Mercado Común del Sur (Mercosur) (Veronese y otros, 2023b: 1315 y 1426). Explican que la RIPD ha evolucionado de un espacio académico a un foro de intercambio de experiencias de políticas públicas, ya que en América Latina se están creando autoridades de protección de datos (Veronese y otros, 2023b: 1315). Además, señalan que Argentina ha dejado de ocupar ese rol central debido a que otras entidades nacionales han comenzado a compartir esa carga. Las entrevistadas mencionan a México y Colombia como miembros influyentes de la RIPD (Veronese y otros, 2023b: 1292 y 1317), y una entrevistada del área académica postula la necesidad de que la RIPD consolide un rol más predominante para que los países latinoamericanos puedan enfrentar dilemas internacionales (Veronese y otros, 2023b: 1297).

27. Autoridade Nacional de Proteção de Dados, «ANPD torna-se membro da Rede Ibero-Americana de proteção de dados», *gov.br*, disponible en https://tipg.link/l8E7.

28. Autoridade Nacional de Proteção de Dados, «ANPD participa de encontro da Rede Iberoamericana de Proteção de Dados», *gov.br*, disponible en https://tipg.link/l8EY.

Como ya se indicó en este texto, la constitucionalización del *habeas data* en Brasil fue un factor influyente en la región. Según un entrevistado del Gobierno argentino, la reforma constitucional de 1994 se inspiró, de manera fundamental, en la Constitución Federal brasileña de 1988 para incluir el *habeas data* (Veronese y otros, 2023b: 1301). Finalmente, una entrevistada del sector académico argentino reitera la información de una evidente influencia de la legislación de ese país sobre este último, como también se señaló por una de las entrevistadas de Uruguay. También menciona la importancia de que los países grandes, en particular Brasil y México, entren en el tema (Veronese y otros, 2023b: 1292).

En relación con México, una entrevistada del Gobierno indica explícitamente que en el país se hace uso de referencias normativas y prácticas de España, Colombia y Chile, a partir de lo que hace hincapié en que siempre hay una búsqueda de estándares internacionales (Veronese y otros, 2023a: 808). La literatura legal sobre la protección de datos personales en México reitera esa información e indica que la apropiación de influencias proviene de España, Alemania y Argentina, ya que la práctica de la protección de datos personales en esos países ha permitido el desarrollo del concepto de autodeterminación informativa (Quijano Decanini, 2022: 165). El INAI de México ha comenzado a tener una participación muy activa en la RIPD, asumiendo un protagonismo evidente (Veronese y otros, 2023a: 632). Varias entrevistadas señalan eso como un factor que justifica la influencia de México en países como Colombia y Chile en el pasado, así como, más recientemente, en Ecuador, Panamá, Nicaragua y El Salvador (Veronese y otros, 2023a: 623, 642, 717, 765 y 770).

Con la excepción de este último país, la mayor influencia de México radicaría en indicar la necesidad de construir autoridades autónomas de protección de datos. El ordenamiento jurídico mexicano reconoce la importancia de establecer que la autoridad no solo es aquella que está reconocida *de iure* y formalmente, perteneciente al Estado, sino también la autoridad *de facto*, que no es parte de la estructura institucional del Gobierno, pero ejerce atribuciones como autoridad autónoma e independiente, garantizando la protección de derechos de datos personales frente al Estado y al sector económico (Hidalgo Rioja, 2018: 50).

El desempeño internacional del INAI es elogiado por muchas entrevistadas (Veronese y otros, 2023a: 595, 682, 699 y 752). En 2023, Australia, Nueva Zelanda, Sudáfrica, Ghana, Túnez y Nepal impulsaron, en el seno de la Conferencia Internacional de Comisionados de Información, un pronunciamiento de respaldo al INAI, en el que se reconoce el papel del organismo garante mexicano como impulsor, promotor y modelo del derecho a saber a nivel internacional.[29]

29. «Recibe INAI respaldo y reconocimiento internacional por su labor», *inai.org*, disponible en https://tipg.link/l-OZ.

Finalmente, cabe destacar que en las entrevistas de Uruguay se mencionó la influencia de los países latinoamericanos a través de la existencia de foros y conferencias, con intercambios e interacciones (Veronese y otros, 2023a: 310). Además, otra entrevistada, del área académica de Uruguay, destacó el conocimiento de los marcos legales y el intercambio directo entre las autoridades de protección de datos personales (Veronese y otros, 2023a: 357). El entorno interamericano también ha influido en la evolución de la ley de protección de datos en Uruguay: la Declaración Americana de los Derechos y Deberes del Hombre de 1948 y la Convención Americana sobre Derechos Humanos de 1968, también conocida como Pacto de San José, reconocieron los derechos a la intimidad y la privacidad como derechos humanos, lo que llevó a su protección en la carta constitucional uruguaya (Durán Martínez, 2012: 22).

La RIPD es señalada como un importante foro de intercambio para la región iberoamericana. La iniciativa surge con el acuerdo alcanzado en el Encuentro Iberoamericano de Protección de Datos celebrado en La Antigua, Guatemala, en junio de 2003, con la asistencia de representantes de catorce países iberoamericanos.[30] Además de los estándares publicados en 2017, en 2020 la RIPD aprobó el Plan Estratégico 2021-2025,[31] que tiene como algunos de sus múltiples objetivos elaborar un marco normativo para la convergencia regional, promover la cooperación efectiva e institucionalizar y profesionalizar las autoridades para reforzar su estabilidad e independencia.

Sobre el espacio del Mercosur, una entrevistada del área académica de Argentina señala que los intentos de cooperación en la práctica entre las autoridades de protección de datos a través de la RIPD, como investigaciones conjuntas, no han tenido éxito, a pesar de que señala la producción de manuales y estudios conjuntos por parte de las autoridades argentinas y uruguayas, los que califica como trabajos académicos más que prácticos (Veronese y otros, 2023b: 1260). La cercanía entre las autoridades de protección de datos de Argentina y Uruguay es clara si se tienen en cuenta los intentos de insertar el tema por medio del Mercosur. En un libro de 2005, investigadores uruguayos ya intentaban debatir sobre la protección de datos personales en relación con los cuatro países de ese bloque económico (Delpiazzo y otros, 2005). En 1999 una investigadora argentina publicó un libro en el que abordó el potencial de esa idea (Slavin, 1999).

Así, es evidente que el tema de la protección de datos personales ha ocupado la agenda del Mercosur en determinados momentos. Uno de ellos fue cuando, en 2010, se firmó un acuerdo con la Unión Europea para el desarrollo del proyecto Mercosur Digital, con el objetivo de fortalecer el tema de la inclusión de la sociedad de la infor-

30. Red Iberoamericana de Protección de Datos, «Quiénes somos», 2025, disponible en https://tipg.link/l-Om.

31. Red Iberoamericana de Protección de Datos, «Plan Estratégico 2021-2025. Red Iberoamericana de Protección de Datos (RIPD)», 2020, disponible en https://tipg.link/lAGb.

mación en el bloque (Travieso, 2014: 1111). A riesgo de sonar repetitivos, vale la pena señalar que una entrevistada de la autoridad de protección de datos de Argentina cree que el tema puede volver con fuerza a la agenda del Mercosur debido a la aprobación de la Ley General de Protección de Datos en Brasil y la creación de la ANPD (Veronese y otros, 2023b: 1334).

El proyecto Mercosur Digital también es mencionado por la autoridad de protección de datos de Uruguay como un medio para establecer un estándar común en el bloque y no para crear una norma de derecho internacional (Veronese y otros, 2023a: 391). El tema, hasta el día de hoy, está presente en los debates del bloque económico, en el seno del Grupo de Agenda Digital (Mercosur, 2023), con especial atención al potencial acuerdo comercial del bloque con la Unión Europea. Ese tema fue objeto de un debate académico en 2019 en la Universidad de Buenos Aires, cuando Eduardo Bertoni aún estaba al frente de la Dirección Nacional de Protección de Datos Personales de la República Argentina.[32]

En este sentido, en la región se está experimentando un proceso social de difusión de la protección de datos personales y la privacidad como un valor social que debe incorporarse en los distintos países. Lo que no existe es una cultura única —y latinoamericana— de protección de datos personales y privacidad debido a las diferencias sociales e institucionales que marcan a los países. Ese proceso en curso encuentra algún foco de propuesta para la armonización de las diferentes culturas jurídicas, ya sean externas o internas. No se puede decir que algún país de la región ofrece mejor o peor protección de los datos personales o de la privacidad que otro. Las sociedades y sus instituciones han dado guarida legal a esos valores, en el límite de sus capacidades y tradiciones en la medida en que los perciben como un conjunto de derechos.

Consideraciones finales

La conclusión que surge del análisis de las sesenta y tres entrevistas y una extensa documentación y literatura es que existe un proceso en marcha en la región a favor de la formación de un concepto social y jurídico latinoamericano de protección de datos personales y privacidad. Este proceso existe en la medida en que se han identificado intercambios evidentes de experiencias y modelos entre los países, ya sea mediante acciones estatales o interacciones con la sociedad civil o empresas. Es muy importante precisar que este artículo no pretende señalar la existencia de una verdad universal o clara sobre el fenómeno completo de la construcción del derecho a la protección de datos personales en Latinoamérica, sino que se basa en informaciones y creencias que son útiles para comprender la visión que los actores sociales involucrados

32. «Acuerdo UE-Mercosur: posibles escenarios en la protección de datos personales», *Derecho al Día*, 18 (330), 14 de noviembre de 2019, disponible en https://tipg.link/l8Ga.

tienen. Esa es la ventaja del uso de entrevistas y su cotejo con la doctrina. Asimismo, es importante señalar que se trata de la primera investigación con profundidad que buscó obtener comparaciones —sin evaluación— para la comprensión de cambios en la región.

Existen pretensiones de construcción de narrativas culturales globales para la protección de la privacidad y los datos personales, mientras que las narrativas nacionales, locales, regionales y de grupos sociales específicos también están aflorando. Esa característica —la coexistencia de narrativas socioculturales— no es específica de esos derechos. No obstante, el fenómeno de la expansión de la digitalización y las nuevas tecnologías de la información ha sido un motor de esas mediaciones.

De ese modo, se observa una interesante construcción paralela (en diferentes momentos y en diferente asignación de recursos) de traducciones de elementos del exterior al interior de los países, que se transforman en prácticas institucionales, sociales y jurídicas específicas, en la medida de los contextos observados. Hay mediaciones e interacciones que pueden hacer una construcción coordinada y cooperativa en el futuro, siempre considerando las diferencias entre los países. Así, aún no existe una cultura latinoamericana única de protección de datos personales y privacidad. Existen varias versiones nacionales y locales de un tipo de derecho que pretende ser amplio, global y, quizás, universal, pero respetando las necesidades locales.

Referencias

Álvarez Robles, Tamara (2022). «Las garantías de los derechos fundamentales en y desde la red: El contexto español. Consideração especial do contexto espanhol». *Revista Chilena de Derecho y Tecnología*, 11 (1): 5-40. DOI: 10.5354/0719-2584.2022.60197.

Álvarez-Valenzuela, Daniel y Alejandro Hevia Angulo (2020). «Protección legal para la búsqueda y notificación de vulnerabilidades de ciberseguridad en Chile». *Revista Chilena de Derecho y Tecnología,* 9 (2): 1-4. DOI: 10.5354/0719-2584.2020.60658.

Álvarez Valenzuela, Daniel y Danielle Zaror Miralles (2022). «Una Constitución digital para Chile». *Revista Chilena de Derecho y Tecnología,* 11 (1): 1-4. DOI: 10.5354/0719-2584.2022.67657.

Arrieta Cortés, Raúl (2009). «Chile y la protección de datos personales: Compromisos internacionales». En *Chile y la protección de datos personales: ¿Están en crisis nuestros derechos fundamentales?* (pp. 18-21). Santiago: Universidad Diego Portales.

Arroyo Kalis, Juan Ángel (2017). «*Habeas data*: Elementos conceptuales para su implementación en México». En Eduardo Ferrer Mac-Gregor y Rogelio Flores Pantoja (coordinadores), *La Constitución y sus garantías: A 100 años de la Consti-*

tución de Querétaro de 1917 (pp. 53-68). Querétaro: Unam. Disponible en https://tipg.link/l8J2.

Basterra, Marcela I. (2008a). *Protección de datos personales: La garantía de* habeas data. Buenos Aires: Ediar.

—. (2008b). *Protección de datos personales: Ley 25326 y Dto. 1558/01 comentados. Derecho Constitucional Provincial: Iberoamérica y México*. Buenos Aires: Ediar.

Benussi Díaz, Carlo (2020). «Obligaciones de seguridad en el tratamiento de datos personales en Chile: Escenario actual y desafíos regulatorios pendientes». *Revista Chilena de Derecho y Tecnología,* 9 (1): 227-279. DOI: 10.5354/0719-2584.2020.56660.

Bordachar Benoit, Michelle (2022). «Comentarios al proyecto de ley chileno sobre protección de datos personales: Deficiencias e inconsistencias en los derechos ARCO». *Revista Chilena de Derecho y Tecnología,* 11 (1): 397-413. DOI: 10.5354/0719-2584.2022.67205.

—. (2023). «Avances legislativos sobre ciberseguridad en Chile». *Revista Chilena de Derecho y Tecnología,* 12: 1-4. Disponible en https://tipg.link/l9-v.

Bustos, Sandra (2018). «Tratamiento de datos personales en el Poder Judicial de Chile: ¿El Gran Hermano jurisdiccional?». *Revista Chilena de Derecho y Tecnología*, 7 (2): 27-44. DOI: 10.5354/0719-2584.2018.49205.

Cervantes Díaz, Fernando (2009). «Derecho a la intimidad y *habeas data*». *Revista Derecho y Realidad,* 7 (13): 27-35. Disponible en https://tipg.link/lA0S.

Choudry, Sujit (2006). *The migration of constitutional ideas*. Cambrige: Cambridge University Press.

Contreras Vásquez, Pablo (2020). «El derecho a la protección de datos personales y el reconocimiento de la autodeterminación informativa en la Constitución chilena». *Estudios Constitucionales,* 18 (2): 87-120. DOI: 10.4067/S0718-52002020000200087.

Contreras Vásquez, Pablo, Michelle Bordachar Benoit y Leonardo Ortiz Mesías (2022). *Privacidad y protección de datos personales jurisprudencia seleccionada y comentada*. Santiago: Der.

De la Calle Restrepo, José Miguel (2009). *Autodeterminación informativa y* habeas data *en Colombia: Análisis de la Ley 1266 de 2008 – Jurisprudencia y derecho comparado*. Bogotá: Temis.

De Oliveira, Caio César (2020). «A Autoridade Nacional de Proteção de Dados e o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade». En Caitlin Mulholand (compiladora), *A LGPD e o novo marco normativo no Brasil* (pp. 371-392). Porto Alegre: Arquipélago.

Delpiazzo, Carlos E., Maricarmen Pascale, Daniela Peña, Flavia Meleras Bekerman y Andrés Saravia Morales (2005). *Protección de datos personales en Uruguay y el Mercosur*. Montevideo: Fundación de Cultura Universitaria.

Doneda, Danilo (2006). *Da privacidade à proteção de dados pessoais*. Río de Janeiro: Renovar.

Durán Martínez, Augusto (2012). *Derecho a la protección de datos personales y al acceso a la información pública*. Montevideo: AMF.

Flórez Ruiz, Rodrigo (2011). *La protección de la intimidad económica con relación al dato financiero en la jurisprudencia constitucional colombiana (1992-2008)*. Medellín: Unaula.

Guerrero Guerrero, Beatriz (2020). «Protección de datos personales en el Poder Judicial: Una nueva mirada al principio de publicidad de las actuaciones judiciales». *Revista Chilena de Derecho y Tecnología*, 9 (2): 33-56. DOI: 10.5354/0719-2584.2020.54372.

Gutiérrez, Andrei (2019). «Da Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade». En Viviane Maldonado, Viviane Nóbrega y Renato Opice Blum (coordinadores), *Lei Geral de Proteção de Dados Comentada* (pp. 439-462). São Paulo: Revista dos Tribunais.

Hidalgo Rioja, Ileana (2018). *Derecho a la protección de datos personales*. Ciudad de México: Instituto de Investigaciones Jurídicas, Secretaría de Cultura e Instituto Nacional de Estudios Históricos de las Revoluciones de México.

Jijena, Renato (2013). «Tratamiento de datos personales en el Estado y acceso a la información pública». *Revista Chilena de Derecho y Tecnología*, 2 (2): 49-94. DOI: 10.5354/0719-2584.2013.30309.

Keller, Clara Iglesias (2019). «Regulação nacional de serviços na Internet: Exceção, legitimidade e o papel do Estado». Tesis de doctorado en Derecho Público de la Universidad del Estado de Rio de Janeiro. Disponible en https://tipg.link/l-P2.

López Carballo, Daniel A. y Francisco Ramón González Calero-Manzanares (coordinadores) (2015). *Protección de datos y* habeas data*: Una visión desde Iberoamérica.* Madrid: Agencia Española de Protección de Datos.

Matus, Jessica (2013). «Derecho de acceso a la información pública y protección de datos personales». *Revista Chilena de Derecho y Tecnología*, 2 (1): 197-228. DOI: 10.5354/0719-2584.2013.26959.

Mendes, Laura Schertel y Gabriel Campos Soares da Fonseca (2020). «STF reconhece direito fundamental à proteção de dados: comentários sobre o referendo da Medida Cautelar nas ADIs 6387, 6388, 6389, 6390 e 6393». *Revista de Direito do Consumidor*, 130: 471-478.

Muñoz, Ana María (2016). «Eliminación de datos personales en internet: El reconocimiento del derecho al olvido». *Revista Chilena de Derecho y Tecnología*, 4 (2): 215-261. DOI: 10.5354/0719-2584.2015.37426.

Muñoz Gutiérrez, Catherine (2021). «La discriminación en una sociedad automatizada: Contribuciones desde América Latina». *Revista Chilena De Derecho y Tecnología*, 10 (1): 271-307. DOI: 10.5354/0719-2584.2021.58793.

Palazzi, Pablo Andrés (1998). «El *habeas data* en el derecho argentino». *Revista Electrónica de Derecho Informático*, 4: 51-92. Disponible en https://tipg.link/lAAR.

—. (2021). «Tutela de derechos personalísimos em internet: el estándar del caso Belén Rodríguez». En Pablo Andrés Palazzi (compilador), *Protección de datos personales: Doctrina y jurisprudencia. Tomo 2* (pp. 129-138). Buenos Aires: Cetys.

Parra Noriega, Luiz Gustavo (2011). «Desarrollo legislativo en materia de datos personales en las entidades federativas: La importancia de una legislación especial en el ámbito estatal». En *Retos de la protección de datos personales en el sector público* (pp. 145-178). Ciudad de México: Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal.

Puccinelli, Oscar R. (2004). *Protección de datos de carácter personal*. Buenos Aires: Astrea.

—. (2014). «El *habeas data* de la Constitución argentina: A veinte años de su inclusión por la Convención Reformadora de 1994». *Pensamiento Constitucional,* 19: 79-109. Disponible en https://tipg.link/lAB5.

—. (2020). «Viejos y nuevos derechos, viejos y nuevos tipos y subtipos de *habeas data*, a propósito de las novedades aportadas por el Reglamento General de Protección de Datos de la Unión Europea y los "Estándares" de la RIPD». En Luis R. Sáenz Dávalos (coordinador), *El* habeas data *en la actualidad: Posibilidades y límites* (pp. 21-74). Lima: Centro de Estudios Constitucionales, Tribunal Constitucional del Perú.

Quijano Decanini, Carmen (2022). *Derecho a la privacidad en internet*. Ciudad de México: Tirant lo Blanch.

Remolina Angarita, Nelson (2015). *Recolección internacional de datos personales: Un reto del mundo post-internet*. Madrid: Agencia Española de Protección de Datos.

Restrepo, Eduardo (2012). *Antropología y estudios culturales*. Buenos Aires: Siglo XXI.

Reusser Monsálvez, Carlos (2021). *Derecho al olvido: La protección de datos personales como límite a las libertades informativas*. Santiago: Der.

Ruiz Ardila, Betsy Yahanna (2016). «Regulación en materia de protección de datos personales o *habeas data* en Colombia por medio de la Ley 1581 de 2012: Examen histórico y crítica sobre su ineficacia ante las administradoras de bases de datos, portales de Internet y motores de búsquedas». Trabajo de grado para obtener la licenciatura en Derecho por la Universidad Católica de Colombia.

Ruiz Martínez, Esteban (2015). *Protección de los datos personales en los informes crediticios: Delitos contra la intimidad informática*. Buenos Aires: Hammurabi.

Saavedra Rionda, Víctor Práxedes, Daniel Ospina Celis, Juan Carlos Upegui Mejía y Diana León (2021). *Desigualdades digitales: Aproximación sociojurídica al acceso a Internet en Colombia*. Bogotá: Dejusticia.

Schuck, Peter H (1999). «¿Por qué los professores de derecho no hacen más investigación empírica?». En Martin F. Böhmer (compilador), *La enseñanza del derecho y el ejercicio de la abogacía* (pp. 129-145). Barcelona: Gedisa.

Simão, Bárbara, Juliana Oms y Livia Torres (2019). *Autoridades de proteção de dados na América Latina: Um estudo dos modelos institucionais da Argentina, Colômbia e Uruguai*. São Paulo: IDEC. Disponible en https://tipg.link/lAIP.

Slavin, Diana (1999). *Mercosur: La protección de datos personales*. Buenos Aires: Depalma.

Travieso, Juan Antonio (2014). *Régimen jurídico de los datos personales. Tomo 2*. Buenos Aires: Abeledo Perrot.

Veronese, Alexandre, Alessandra Silveira, Amanda Braga, Amanda Nunes Lopes Espiñeira Lemos, Eduarda Costa Almeida, Luiza Mendonça da Silva Belo Santos, Luiza Peixoto Veiga, Mariana Moutinho Fonseca, Marcio Iorio Aranha, Rebecca Lemos Igreja, Thiago Guimarães Moraes y Vitória Bragança Sernégio (2023a). *Pesquisa documental e de campo sobre autoridades de proteção de dados na América Latina: O conceito social e institucional de privacidade e de dados pessoais: Anexo 2 (encuestas no identificadas). Volume 1*. Brasilia: Fapesp. DOI: 10.13140/RG.2.2.18785.83042

—. (2023b). *Pesquisa documental e de campo sobre autoridades de proteção de dados na América Latina: o conceito social e institucional de privacidade e de dados pessoais: Anexo 2 (encuestas no identificadas). Volume 2*. Brasilia: Fapesp.. DOI: 10.13140/RG.2.2.32207.60321

Zegarra Valdivia, Diego (2019). «La normativa peruana de protección de datos personales frente al reto de pasar de un modelo de gestión de datos al uso responsable de la información». En Diego Zegarra Valdivia (coordinador), *La proyección del derecho administrativo peruano: Estudios por el Centenario de la Facultad de Derecho de la PUCP* (pp. 165-210). Lima: PUCP.

Sobre los autores

Alexandre Veronese es licenciado en Derecho por la Universidad Federal de Río de Janeiro, tiene una maestría en Derecho y Sociología por la Universidad Federal Fluminense y un doctorado en Sociología por el Instituto de Estudios Sociales y Políticos de la Universidad Estatal de Río de Janeiro. Actualmente, es profesor asociado de Teoría Social y Derecho en la Universidad de Brasilia e investigador del Centro de Política, Derecho, Economía y Tecnologías de la Comunicación de la misma universidad. Es coordinador del Grupo de Estudios de Derecho de las Telecomunicaciones

en la Universidad de Brasilia e investigador asociado del Centro de Estudios de Derecho de la Unión Europea de la Universidad de Minho, Portugal. Imparte docencia e investigación en teoría social y derecho, y en derecho, tecnología e innovación. Su correo electrónico es veronese@ccom.unb.br. 0000-0002-2287-1005.

Rebecca Lemos Igreja es antropóloga, magíster en antropología por el Centro de Investigaciones y Estudios Superiores en Antropología Social de México, y doctora en Antropología y Estudios Latinoamericanos por la Universidad de Brasilia. Actualmente, es secretaria general de la Facultad Latinoamericana de Ciencias Sociales y profesora del Instituto de Ciencias Sociales y del Programa de Posgrado de la Facultad de Derecho de la Universidad de Brasilia. Es también profesora del Instituto Rio Branco del Ministerio de Relaciones Exteriores de Brasil y profesora asociada en el Centre D'étude Des Mouvements Sociaux del École Des Hautes Études En Sciences Sociales en Francia. Su correo electrónico es rebecca.igreja@gmail.com. 0000-0002-9533-2985.

Marcio Iorio Aranha tiene una maestría y un doctorado por la Universidad de Brasilia con una estancia postdoctoral en la University of Southern California. Es profesor de Derecho Constitucional y Administrativo en la Facultad de Derecho de la Universidad de Brasilia, donde es director ejecutivo del Núcleo de Derecho Sectorial y Regulatorio y preside el cuerpo editorial del *Journal of Law and Regulation* y de la *Revista de Derecho, Estado y Telecomunicaciones*. Su correo electrónico es iorio@unb.br. 0000-0001-9436-0987.

Amanda Nunes Lopes Espiñeira Lemos es abogada, licenciada por la Universidad Federal de Bahía, magíster por la Universidad de Brasilia y doctora en Derecho por la misma universidad, en régimen de cotutela con la Universidad de Minho, Portugal. Actualmente, es asesora legislativa y becaria en proyectos de investigación con la Fundación Oswaldo Cruz y la Universidad de Brasilia, como investigadora colaboradora del Centro de Política, Derecho, Economía y Tecnologías de la Comunicación. Es investigadora junior del Centro de Investigación en Justicia y Gobernanza de la Universidad del Miño, Portugal. Su correo electrónico es amandaespineira@ccom.unb.br. 0000-0002-7114-4613.

Mariana Moutinho Fonseca tiene una maestría en Derecho por la Universidad de Connecticut y en Derecho, Estado y Constitución por la Universidad de Brasilia. Actualmente trabaja como defensora pública federal y hace doctorado en derecho en la Universidad de Brasilia. Fue especialista en regulación de servicios de telecomunicaciones en la Agencia Nacional de Telecomunicaciones. Su correo electrónico es mariana-moutinho@hotmail.com. 0009-0003-6270-7618.

Luiza Mendonça da Silva Belo Santos es máster en Derecho, Estado y Constitución por la Universidad de Brasilia, donde también obtuvo su título de grado en Derecho. Actualmente, trabaja como abogada especializada en tecnología, protección de datos y ciberseguridad, ofreciendo asesoría en gobernanza de datos, privacidad y

riesgos legales asociados a la innovación. Su correo electrónico es luiza.mendonca.s@hotmail.com. 0000-0003-0517-2023.

Luiza Veiga es magíster en Derecho por la Universidad de Brasilia. Se desempeña como asesora de juez en el Tribunal Regional Federal. Su correo electrónico es luiza.pveiga@hotmail.com. 0000-0001-7563-3337.

Amanda Braga Ferreira es abogada, licenciada en Derecho por la Universidad de Brasilia, con movilidad internacional en la Facultad de Derecho de la Universidad de Lisboa. Actualmente, hace doctorado en Derecho en la Universidad de Brasilia. Es integrante del Grupo de Estudios en Derecho de las Telecomunicaciones y se desempeña como asesora en la Secretaría de Relaciones Institucionales de la Presidencia de la República de Brasil. Su correo electrónico es amandaabrf@gmail.com. 0009-0002-8800-2029.

Vitória Sernégio es abogada con actuación en derecho regulatorio y contratos, licenciada por la Universidad de Brasilia y especialista en tribunales superiores. Es investigadora en el Grupo de Estudios sobre Constitución, Empresa y Mercado de la Universidad de Brasilia. Su correo electrónico es vitoriabsernegio@gmail.com. 0009-0001-5035-0426.

Alessandra Silveira es doctora en Ciencias Jurídico-Políticas por la Universidad de Coimbra. Actualmente, es profesora asociada (con agregación) en la Escola de Direito da Universidade do Minho, Portugal, directora del máster en Derecho de la Unión Europea en la misma universidad y coordinadora del Centro de Excelencia Jean Monnet sobre Ciudadanía Digital y Sostenibilidad Tecnológica. Es titular de la Cátedra Jean Monnet en Derecho de la Unión Europea y directora y fundadora de *Unio– EU Law Journal* y de su blog oficial *Thinking and debating europe*. También es profesora visitante en la Università degli Studi di Verona, Italia, la Universidade de Brasília, la Universidade de Santa Cruz do Sul y la Universidade do Extremo Sul Catarinense, Brasil. Su correo electrónico es asilveira@direito.uminho.pt. 0000-0001-5246-7954.

Thiago Guimarães Moraes es candidato a doctorado en Derecho por la Universidad de Brasilia y la Vrije Universitet Brussel, y becario de doctorado del grupo de Gobernanza Digital del Instituto de Estudios Comparativos Regionales Integrados de la Universidad de las Naciones Unidas. Tiene un máster en Derecho y Tecnología por la Universidad de Tilburg, una maestría en Ciencias de la Información y dos licenciaturas, una en Derecho y otra en Ingeniería de Redes, ambas por la Universidad de Brasilia. Actualmente, trabaja como especialista en protección de datos y gobernanza de inteligencia artificial en la Autoridad Nacional de Protección de Datos. Es cofundador y consejero del Laboratorio de Políticas Públicas e Internet. Su correo electrónico es moraes.t@gmail.com. 0009-0000-3873-3865.

Eduarda Costa es abogada y licenciada en Derecho por la Universidad de Brasilia. Es monitora del programa de posgrado en Derecho Digital y Protección de Datos del Instituto Brasiliense de Direito Público e investigadora del Laboratorio de Privacidad del Centro de Direito, Internet e Sociedade del del Instituto Brasiliense de Direito Público. Su correo electrónico es itseduardacosta@gmail.com. 0000-0002-0575-611X.

REVISTA CHILENA DE DERECHO Y TECNOLOGÍA

La *Revista Chilena de Derecho y Tecnología* es una publicación académica semestral del Centro de Estudios en Derecho, Tecnología y Sociedad de la Facultad de Derecho de la Universidad de Chile, que tiene por objeto difundir en la comunidad jurídica los elementos necesarios para analizar y comprender los alcances y efectos que el desarrollo tecnológico y cultural han producido en la sociedad, especialmente su impacto en la ciencia jurídica.

DIRECTOR
Daniel Álvarez Valenzuela
(dalvarez@derecho.uchile.cl)

SITIO WEB
rchdt.uchile.cl

CORREO ELECTRÓNICO
rchdt@derecho.uchile.cl

LICENCIA DE ESTE ARTÍCULO
Creative Commons Atribución Compartir Igual 4.0 Internacional

La edición de textos, el diseño editorial
y la conversión a formatos electrónicos de este artículo
estuvieron a cargo de Tipográfica
(www.tipografica.io).