Naciones Unidas A/HRC/49/55

Asamblea General

Distr. general
13 de enero de 2022

Original: español

Consejo de Derechos Humanos
49º período de sesiones
28 de febrero a 1 de abril de 2022
Tema 3 de la agenda
Promoción y protección de todos los derechos humanos, civiles, políticos, económicos, sociales y culturales, incluido el derecho al desarrollo

La privacidad y la protección de datos personales en Iberoamérica: ¿un paso hacia la globalización?

Informe de la Relatora Especial sobre el derecho a la privacidad, Ana Brian Nougrères

Resumen

Iberoamérica ha experimentado una evolución harto interesante en materia de privacidad y protección de datos personales desde los albores del siglo XXI.

El presente informe versa sobre la situación actual en Iberoamérica respecto a la privacidad desde la perspectiva de la protección de datos personales, sus antecedentes y su enfoque internacional. En el informe se realiza un análisis de la cuestión partiendo de la evolución del sistema uruguayo en los últimos 20 años. Se describe también su proceso evolutivo en relación con el resto de los países iberoamericanos y, por último, se analiza cómo se han encauzado los sistemas de protección de datos personales en los últimos años para conformar el sistema iberoamericano de protección de datos personales.

La Relatora Especial plantea que el objeto de estudio del presente informe puede constituirse en un ejemplo de una forma de trabajo de consuno hacia un mundo en el que los principios en materia de privacidad y protección de datos personales sean consensuados y respetados y lleven a implementar estándares de privacidad digital, y en el que la integración y la armonización se constituyan en desafíos alcanzables, siempre siguiendo una concepción ética que respete las diversidades de los pueblos.

I. Introducción

1. La doctrina que ampara la privacidad y la protección de datos personales es consecuencia de la creciente preocupación por el avance de las tecnologías de la información y la comunicación, que vienen a proveer de una posibilidad de gerenciamiento y manipulación de la información cada vez mayor, con potencialidades para atentar contra la libertad, la vida y la dignidad de las personas.

2. La tecnología ha evolucionado de forma tal que ha llevado a conformar un nuevo diseño del mundo y de las formas de comunicación, socialización, educación y trabajo, así como una nueva manera de encarar los problemas de salud, la cultura y el desarrollo social. En esta coyuntura, la doctrina de la privacidad y la protección de datos personales, en cuanto que derechos fundamentales de las personas, tienen en la actualidad mayor trascendencia para la dignidad humana de lo que tenían históricamente, fomentando la autonomía, la toma de decisiones, la innovación y, en definitiva, el desarrollo de la propia personalidad humana.

3. La inteligencia artificial, la tecnología de cadena de bloques, la rapidez en el procesamiento de la información, la realidad virtual, la realidad aumentada, la biotecnología, la robótica, el Internet de las cosas, la videovigilancia masiva y las impresiones tridimensionales constituyen fenómenos disruptivos que traen consigo transformaciones profundas en la forma de afrontar la vida diaria.

4. La pandemia, además, no solo ha acelerado los procesos de digitalización, sino que también ha llevado a volcar las vidas de las personas hacia una mayor integración con las tecnologías y esto, a la vez que denota grandes ventajas, trae aparejados riesgos graves, en especial en lo que concierne a la seguridad de la información, la privacidad y el manejo de datos personales.

5. En este contexto, es preciso tener siempre presente que la persona es el centro de todo universo normativo y que la consagración de los derechos humanos fundamentales es un elemento esencial para el desarrollo de la personalidad en las sociedades democráticas. El reconocimiento y la protección de los derechos humanos fundamentales habrán de tender siempre a hacer más plena la vida de las personas, considerando en todo momento al ser humano como el centro del estado de derecho.

6. Proteger la privacidad y los datos personales de los individuos es, además, atender a su dignidad, su igualdad y su libertad, y es también trabajar en pos de una sociedad más igualitaria en la que la intimidad no sea un privilegio de unos pocos.

7. El derecho a la privacidad y, en especial, el derecho a la protección de datos personales se presentan como formas de proteger a las personas otorgándoles medios para hacer valer su autonomía y su dignidad en forma igualitaria. Estos derechos requieren, como todos los derechos, de una garantía a nivel jurisdiccional que sea efectiva. En la medida en que garantizan la capacidad de las personas para comunicar y compartir, estos derechos constituyen elementos determinantes tanto para la existencia de una sociedad democrática como para su plena funcionalidad.

8. Las normas en la materia vienen a ejercer cual garantías para el individuo en el ejercicio de sus derechos fundamentales, otorgando medios para la protección de la privacidad, la dignidad, la igualdad y, en definitiva, la libertad de las personas. En especial, el derecho a la protección de datos personales es un elemento esencial para el desarrollo de la personalidad en las sociedades democráticas, así como para la existencia y el funcionamiento de una sociedad democrática. Tiene por finalidad propender a un flujo controlado de datos personales, a la vez que fomentar el comercio.

II. El sistema iberoamericano: antecedentes

9. La mayor parte de los países iberoamericanos ya poseían en los albores del siglo XXI sistemas de protección de datos que, en términos generales, eran muy diferentes de los actuales en la medida en que no reconocían expresamente el derecho a la protección de datos personales, aunque algunas constituciones, como, por ejemplo, la Constitución de Colombia de 1991, modificada en 2003, ya regulaban acerca de la privacidad.

10. Si se toma el caso del Uruguay, que sigue este lineamiento general iberoamericano, se observa que el derecho humano fundamental a la protección de datos personales ha tenido siempre un estatuto de protección en el ordenamiento jurídico, aunque sufrió variaciones sustanciales, como se verá en los capítulos siguientes.

11. La Constitución del Uruguay —siguiendo una tendencia que se repite en Iberoamérica— se afilia a un sistema de protección de la privacidad y de los datos personales que, al reconocer la no taxatividad de los derechos constitucionales, admite que la enumeración de derechos, deberes y garantías no excluye otros que son inherentes a la personalidad humana o se derivan de la forma republicana de gobierno.

12. En efecto, si bien el derecho a la intimidad no tiene consagración específica en la Constitución del Uruguay, en su artículo 7º se especifica el derecho de sus habitantes a ser protegidos en el goce de su vida, honor, libertad, seguridad, trabajo y propiedad, y se establece que nadie puede ser privado de estos derechos sino conforme a las leyes que se establecen por razones de interés general.

13. Tomando como base el mencionado artículo 7º de la Constitución del Uruguay, la doctrina de ese país distingue una primera clase de derechos fundamentales que son reconocidos por la Constitución, preexistentes a dicho cuerpo normativo e inherentes a todos los habitantes del país en cuanto individuos de la especie humana (libertad, vida, honor, seguridad, trabajo y propiedad), de una segunda clase de derechos consagrados constitucionalmente a favor del individuo que en su esencia constituyen el derecho a ser protegidos en el goce de cada uno de los derechos preexistentes y que nacen por la propia regulación que de ellos hace el cuerpo normativo.

14. Esta noción se funda en tres artículos de la Constitución del Uruguay: el artículo 7º, ya mencionado, y los artículos 72 y 332. Estos artículos vienen a conciliar una concepción iusnaturalista de la Constitución del Uruguay al reconocer la existencia de derechos que son anteriores pero que no requieren ser creados normativamente y que no dejarán de aplicarse por el hecho de que no exista reglamentación específica. La falta de reglamentación específica será suplida recurriendo a los fundamentos de leyes análogas, los principios generales de derecho y las doctrinas generalmente admitidas.

15. En tal sentido cabe mencionar el derecho de acceso, la privacidad y la protección del dato de carácter personal, que en ese momento no tenían reconocimiento legal expreso.

16. Ahora bien, todos los derechos de las personas requieren de garantías efectivas y estas no son provistas de manera automática por la sola consagración normativa de los derechos.

17. Cabe preguntarse cuál es el límite de esta prerrogativa constitucional y ha de entenderse que lo es el principio de legalidad, conforme al cual el límite viene dado por la ley dictada por razones de interés general.

18. Esta concepción de la Constitución del Uruguay sí consagra los derechos humanos fundamentales, pero la mera consagración constitucional se presenta carente de los elementos de garantía adecuados para la protección de un derecho humano fundamental inherente a la privacidad y a la protección de datos personales y a la dignidad, mientras estos derechos no tenían una consagración genérica explícita en el ordenamiento jurídico positivo del país. Esto implica que existían límites para un adecuado ejercicio de los derechos y para ejercer las garantías que pretenden hacer efectivos los derechos.

19. Ante la necesidad de dar concreción a las disposiciones programáticas de la Constitución que refieren a principios generales del derecho y, en la medida en que estos comprenden los derechos humanos fundamentales a la privacidad y a la protección de datos personales, adquiere relevancia el análisis de los pactos, convenciones y declaraciones de carácter internacional que les dan forma.

20. Sin pretender hacer un estudio pormenorizado de los instrumentos internacionales, son trascendentes en la materia, en principio, el Pacto Internacional de Derechos Civiles y Políticos, aprobado por la Asamblea General de las Naciones Unidas en su resolución 2200 A (XXI), de 16 de diciembre de 1966[1]; la Convención Americana sobre Derechos Humanos:

[1] Artículo 17.

"Pacto de San José de Costa Rica"[2]; la Declaración Universal de Derechos Humanos, proclamada por la Asamblea General de las Naciones Unidas en su resolución 217 A (III), de 10 de diciembre de 1948[3]; el Convenio sobre la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, aprobado por el Consejo de Europa en 1981 y modernizado en 2018; las Directrices de la Organización de Cooperación y Desarrollo Económicos sobre la protección de la privacidad y flujos transfronterizos de datos personales, aprobadas en 1980 y enmendadas en 2013; y la resolución 45/95 de la Asamblea General de las Naciones Unidas, de 14 de diciembre de 1990, entre otras.

21. Entre los instrumentos regionales relevantes en América se encuentran también los Estándares de Protección de Datos Personales para los Estados Iberoamericanos aprobados por la Red Iberoamericana de Protección de Datos en 2017.

22. Cabe preguntarse cuál es la jerarquía de los tratados internacionales en los ordenamientos jurídicos.

23. En el caso de la Argentina, la propia Constitución en su artículo 75, numeral 22, otorga jerarquía constitucional a los tratados internacionales de derechos humanos. En el mismo artículo, en su numeral 23, se determina la potestad del Congreso de generar medidas de acción positiva para garantizar el pleno goce y ejercicio de los derechos reconocidos en tratados internacionales.

24. En el caso del Uruguay, la norma que ratifica un tratado tiene jerarquía de ley. No existe un texto expreso que otorgue jerarquía a los tratados internacionales. No obstante, doctrinariamente se sostiene que los derechos, deberes y garantías previstos en tratados internacionales pueden incorporarse al derecho interno con jerarquía constitucional por ser inherentes a la personalidad humana o derivar de la forma republicana de gobierno y entrar por tanto en la definición del artículo 72 de la Constitución. Esta consideración es trascendente, pues obliga a una necesaria armonización del derecho interno con el emanado de fuentes internacionales en materia de privacidad y protección de datos personales.

25. Muchos países iberoamericanos basaban sus sistemas de protección de datos en disposiciones normativas que se vieron complementadas con desarrollos jurisprudenciales que vinieron a llenar vacíos y a desarrollar principios esenciales (Costa Rica), mientras que otros basaban sus sistemas en normativas sectoriales (Chile[4] y el Perú[5]), complementadas con disposiciones marco que amparaban la protección de datos personales y el derecho de acceso, con mayor o menor grado de explicitación, según los casos.

26. Otros marcos normativos definían datos sensibles, como es el caso del artículo 4º de la Ley núm. 1682/2001 del Paraguay.

27. Algunos sistemas regulan el requerimiento del consentimiento expreso, como es el caso de la Argentina, mediante el artículo 5º de la Ley núm. 25.326 y el artículo 5º del Decreto núm. 1558/2001, que constituyó un caso aislado de regulación del dato personal en Iberoamérica desde 2001 hasta 2008, cuando el Uruguay consolidó su sistema de protección de datos, siguiendo así ambos países el modelo del sistema europeo de protección.

28. La acción de *habeas data* en algunas constituciones iberoamericanas tiene consagración explícita, como es el caso de las del Brasil[6], el Paraguay[7] y el Ecuador[8], mientras que en las de Portugal[9] y Colombia[10] se reconoce la acción tácitamente junto con elementos

[2] Artículo 11.
[3] Artículo 12.
[4] Ley Orgánica Constitucional de Bases Generales de la Administración del Estado y Decreto con Fuerza de Ley núm. 1/19.653, de 2001, del Ministerio Secretaría General de la Presidencia de Chile.
[5] Ley núm. 27489/2001, de junio de 2001, que Regula las Centrales Privadas de Información de Riesgos y de Protección al Titular de la Información.
[6] Artículo 5 (LXXII) de la Constitución Política de la República Federativa del Brasil de 1988.
[7] Artículo 135 de la Constitución de la República del Paraguay de 1992.
[8] Artículo 92 de la Constitución del Ecuador de 2008.
[9] Artículo 35 de la Constitución de Portugal de 1976.
[10] Artículo 15 de la Constitución Política de Colombia de 1991.

propios de la protección de datos personales. En el Brasil[11] y México[12] se reconoce el derecho de acceso.

29. Con la introducción de la acción de *habeas data* se configuran algunos sistemas de garantías más efectivos y actualizados, aunque en general todos han ido superándose con el advenimiento del nuevo sistema de protección de datos personales iberoamericano que ha ido tomando forma en los últimos años.

30. En términos generales, los sistemas normativos de los países iberoamericanos ya habían establecido a finales del siglo XX que, como se explicara para el caso del Uruguay, aun a falta de una disposición que expresamente regulase los temas de privacidad y protección de datos personales o el *habeas data*, existía un estatuto constitucional en la materia, el amparo a este derecho humano fundamental se encontraba presente y era adecuado en tanto en cuanto tiene por fundamento una concepción iusnaturalista de los derechos humanos, como en lo que concierne a la filosofía que inspira el articulado que se analizó *supra*.

31. Ahora bien, en varios países el sistema tenía su fallo al momento de concretar las disposiciones programáticas de las constituciones en el intento de efectivizar disposiciones que referían a los principios generales del derecho de una manera comprensiva de los derechos humanos a la dignidad, la protección de datos personales y la privacidad.

32. Completaban el panorama las disposiciones sectoriales que algunos países aprobaron en materia de datos en salud, datos estadísticos, datos de los niños, registros crediticios o secreto profesional, entre otros.

III. El sistema iberoamericano: hitos hacia la transformación

33. Fueron tres los hitos que marcaron el proceso que culminara en el desarrollo de la legislación iberoamericana en materia de protección de datos personales.

34. El primero fue la Declaración de la XIII Cumbre Iberoamericana de Jefes de Estado y de Gobierno de Santa Cruz de la Sierra (Estado Plurinacional de Bolivia), de noviembre de 2003, que en su considerando 45 establece lo siguiente: “somos conscientes de que la protección de datos personales es un derecho fundamental de las personas y destacamos la importancia de las iniciativas regulatorias iberoamericanas para proteger la privacidad de los ciudadanos contenidas en la Declaración de La Antigua por la que se crea la Red Iberoamericana de Protección de Datos, abierta a todos los países de nuestra Comunidad”.

35. En términos similares, en la Declaración Final adoptada en la 27ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, celebrada en Montreux (Suiza) en septiembre de 2005, nuevamente se reconoció a nivel global la importancia de las actividades de esta Red.

36. El segundo hito lo constituye la Declaración de La Antigua (Guatemala) con motivo del II Encuentro Iberoamericano de Protección de Datos Personales celebrado en junio de 2003, que fue adoptada por los representantes de la Argentina, el Brasil, Chile, Colombia, Costa Rica, el Ecuador, El Salvador, España, Guatemala, México, Nicaragua, el Paraguay, el Perú, Portugal y el Uruguay, en especial cuando sus miembros establecen que:

> “1º Valoran el creciente interés, preocupación y compromiso que en el ámbito de los países iberoamericanos se ha puesto de manifiesto con la protección de datos personales.
>
> 2º Reiteran la consideración de la protección de datos personales como un auténtico derecho fundamental de las personas, sobre todo en orden al respeto a su intimidad y de su facultad de control y disposición sobre los mismos.
>
> [...]

[11] Ley núm. 9.507 del Brasil, de 1997.

[12] Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental de México, de 11 de junio de 2002.

> 5º Constatan la necesidad de impulsar la adopción de medidas que garanticen un elevado nivel de protección de datos, así como la idoneidad de contar con marcos normativos nacionales que, inspirados en tradiciones jurídicas comunes, en el respeto a los derechos fundamentales y en los intereses de sus respectivos países, garanticen una protección adecuada en todos los países iberoamericanos. Tales marcos normativos deberían tomar en consideración los principios esenciales de protección de datos reconocidos en los instrumentos nacionales. En este sentido, consideran muy positivas las iniciativas regulatorias que se han puesto en marcha en diversos países iberoamericanos.
>
> 6º Resaltan la importancia de potenciar las iniciativas de intercambio de experiencias entre los países iberoamericanos, estableciendo canales permanentes de diálogo y colaboración en materia de protección de datos.
>
> 7º Con este fin, y al objeto de reforzar la mutua y continua colaboración entre ellos, avanzando en base al Foro Permanente creado con ocasión del Primer Encuentro, se constituyen en la Red Iberoamericana de Protección de Datos [...], abierta a la incorporación de representantes de todos los países iberoamericanos.
>
> [...]
>
> 8º Son conscientes de que el derecho a la protección de datos personales fortalece el estado de derecho y ayuda a reforzar la democracia en los países iberoamericanos, así como su prestigio y credibilidad en un mundo globalizado. A tal fin, y en el marco legal e institucional de sus respectivos países, realizarán, dentro de sus respectivas competencias, los esfuerzos necesarios para que la protección de datos personales sea impulsada en el seno de la Conferencia Iberoamericana, en la certeza de que así se promoverá la difusión y concienciación de tan importante derecho fundamental."

37. El tercer hito es la Declaración de Cartagena de Indias (Colombia), de 2004, que, en consideración a la importante función informativa de la Red Iberoamericana de Protección de Datos, que es útil para entender cómo opera la protección de datos en cada país, decide asumir una actitud más proactiva en procura de logros más concretos tendientes al intercambio de información relevante en la materia, a la creación de un consejo permanente de asistencia recíproca y a la cooperación en la creación de documentos o propuestas en común. Surgieron así entonces, y en los años siguientes, documentos sobre protección de datos en el sector financiero (Cartagena de Indias, 2004); transferencias internacionales de datos: perspectivas europeas e iberoamericanas (Cartagena de Indias, 2004); el sector de las telecomunicaciones e Internet ante los ataques de la privacidad (Cartagena de Indias, 2004); el sector comercial y el uso de la información con fines de *marketing* (Cartagena de Indias, 2004); viabilidad de la creación de autoridades de control en el entorno latinoamericano (México, 2005); gobierno electrónico y telecomunicaciones (México, 2005); acceso a la información pública y protección de datos (México, 2005); impulso normativo y armonización (Santa Cruz de la Sierra, 2006); la Red "on-line" (Santa Cruz de la Sierra, 2006); instrumentos de autorregulación (Santa Cruz de la Sierra, 2006); tratamiento de datos en salud en relación con la historia clínica (Santa Cruz de la Sierra, 2006); y directrices para la armonización de la regulación de la protección de datos en la comunidad iberoamericana (Cartagena de Indias, 2007). Esta forma de actuación de la Red Iberoamericana está presente hasta nuestros días, y en tal sentido pueden consultarse en su sitio web los siguientes documentos: Recomendaciones de la Red Iberoamericana de Protección de Datos para el tratamiento de datos personales sobre la salud en tiempos de pandemia (2021), Recomendaciones para el tratamiento de datos personales mediante servicios de computación en la nube (2021), Declaración de la Red Iberoamericana de Protección de Datos contra la Violencia Digital en Mujeres y Niñas (2021), Recomendaciones Generales para el Tratamiento de Datos en la Inteligencia Artificial (2019), Orientaciones Específicas para el Cumplimiento de los Principios y Derechos que Rigen la Protección de los Datos Personales en los Proyectos de Inteligencia Artificial (2019) y Estándares de Protección de Datos Personales para los Estados Americanos (2017).

IV. El sistema iberoamericano: su evolución

38. Los sistemas jurídicos para la protección de datos personales están conformados por un conjunto de principios que honran la privacidad y la adecuada forma de proteger los datos personales, teniendo en cuenta también la importancia de fomentar los flujos de la economía. Incluyen la reglamentación de derechos y acciones del titular de los datos, y regulan el consentimiento, las responsabilidades, la protección diferencial, la seguridad, las autoridades de protección de datos y las sanciones, entre otros aspectos.

39. La forma de organizar estos distintos elementos conforma diferentes sistemas. Así, se pueden analizar sistemas basados en la autorregulación o en normas sectoriales. Se constata que algunos sistemas se apoyan en autoridades de protección, mientras que otros no tienen en sus organigramas ese tipo de autoridades de actuación proactiva y preventiva. Se observa también que existen modelos de corregulación que cuentan con la participación de empresas, industrias, comercio, el Estado, usuarios y agencias de contralor a fin de generar ámbitos de análisis y tomas de decisiones óptimas.

40. En Iberoamérica se puede apreciar que la mayoría de los países consideran en sus constituciones el derecho a la privacidad un derecho fundamental, como se ha explicado en el capítulo II *supra*.

41. En cuanto a la protección de datos personales, que es también un derecho humano fundamental, mucho se ha avanzado en el correr de las últimas dos décadas, evolucionando hacia la promulgación de leyes que se basan en el sistema europeo de protección de datos.

42. Esto implica la existencia de una ley general sobre protección de datos personales, además de una serie de principios que han de honrarse, entre los cuales están el principio del consentimiento, como base legitimadora del tratamiento de los datos, y el principio de la finalidad, que marca los límites del consentimiento legal, así como obligaciones, derechos y responsabilidades de los distintos sujetos en juego. Se establece la necesaria participación de una autoridad de control, que debe ejercer sus funciones con autonomía y puede ejercerlas *ex ante* en forma preventiva y establecer sanciones *ex post* para el caso de incumplimiento. Es de estilo asimismo que todo sistema de protección de datos contenga instrumentos jurídicos para garantizar los derechos en forma administrativa y judicial, que normalmente se verán complementados por mecanismos de seguridad informática.

43. A finales del siglo pasado no se apreciaban en Iberoamérica países cuyos cuerpos legislativos consagraran la protección de datos personales con carácter general, con las excepciones de Chile (Ley núm. 19.628, de 1999) y la Argentina (Ley núm. 25.326, de 2000), además de los casos de España y Portugal, que se presentaban liderando el movimiento de transformación desde la Unión Europea. La protección de datos personales en los demás países de Iberoamérica era concebida teniendo por base la concepción iusnaturalista de las constituciones nacionales, y la defensa del derecho provenía de la interpretación armónica de las mismas con los tratados internacionales y algunas disposiciones de derecho interno que fueran aplicables. A su vez, algunas disposiciones sectoriales aprobadas en los distintos países venían a completar el régimen en la materia.

44. Poco a poco, la iniciativa de seguir el modelo que fuera propuesto en 2003 en la XIII Cumbre Iberoamericana de Jefes de Estado y de Gobierno de Santa Cruz de la Sierra y en la Declaración de La Antigua fue objeto de análisis y difusión por parte de la Red Iberoamericana de Protección de Datos y se fue transformando en tendencia.

45. En tal sentido, los países iberoamericanos que fueron adoptando el modelo de ley que abarca los datos personales en forma integral son el Uruguay, desde 2008[13]; México, a partir

[13] Ley núm. 18331, de agosto de 2008.

de 2010[14]; el Perú[15] y Costa Rica[16], desde 2011; Nicaragua[17] y Colombia[18], desde 2012; Panamá[19], desde 2019; el Brasil[20], que aprobó su ley en 2018; y el Ecuador[21], que lo hizo en 2021.

46. En cuando a la autoridad de protección de datos, la ley brasilera la constituye como un órgano de la Administración Pública Federal indirecta que integra la Presidencia de la República[22]. En el Ecuador, mediante el artículo 75 de la Ley Orgánica de Protección de Datos Personales, se crea la Autoridad de Protección de Datos Personales, que es pública e independiente y tiene a su cargo la supervisión de la ley. En Nicaragua, mediante los artículos 28 y 29 de la Ley núm. 787/2012, se crea la Dirección de Protección de Datos Personales adscripta al Ministerio de Hacienda y Crédito Público, con la finalidad de controlar, supervisar y proteger los datos personales en bases públicas y privadas. El Paraguay posee una ley de protección de datos personales crediticios[23] que otorga potestades en la materia a dos autoridades: el Banco Central y la Secretaría de Defensa del Consumidor y el Usuario. La autoridad correspondiente en el Uruguay[24], la Unidad Reguladora y de Control de Datos Personales, es un desconcentrado de la agencia de gobierno electrónico del país, unidad ejecutora de la Presidencia de la República. La autoridad panameña en materia de protección de datos es la Autoridad Nacional de Transparencia y Acceso a la Información, que al efecto se informa a través del Consejo de Protección de Datos Personales, que tiene una integración multisectorial de nueve miembros. Colombia[25], por su parte, radica en la Delegatura para la Protección de Datos Personales de la Superintendencia de Industria y Comercio el ejercicio de la vigilancia para garantizar que en el tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos de la ley.

47. En todos los casos se trata de autoridades de control que tienen un mayor o menor grado de autonomía en el organigrama funcional del Estado y que se presentan con autonomía técnica, aunque no tienen autonomía presupuestaria.

48. En tal sentido, la Argentina actualmente presenta una situación diferenciada de la del resto de Iberoamérica. Si bien en 2000 tuvo a la autoridad de protección de datos personales radicada en el Ministerio de Justicia, en 2017, por Decreto de Necesidad y Urgencia, la autoridad nacional de protección de datos cambió su grado de autonomía, incorporándose como función del Jefe de Gabinete de Ministros la de garantizar el efectivo ejercicio del derecho de acceso a la información pública y controlar la aplicación de la Ley de Protección de Datos Personales. En el mismo año se creó la Agencia de Acceso a la Información Pública, a la que se le asignó la función de fiscalizar la protección integral de los datos personales para garantizar el derecho al honor y a la privacidad de las personas[26]. Los cometidos referidos a la protección de datos, por lo tanto, quedaron subsumidos a partir de 2017 entre las competencias de la Agencia de Acceso a la Información Pública.

49. En lo que concierne a las transferencias internacionales de datos, estas se encuentran, en principio, prohibidas conforme al sistema europeo de protección de datos personales. Siendo el sistema europeo de protección de datos el más exigente, admite el reconocimiento a determinados países del estatus de "adecuación", que implica que tanto la normativa de terceros países como su aplicación práctica se adaptan al sistema de la Unión Europea y, por

[14] Ley Federal de Protección de Datos Personales en Posesión de los Particulares, Ley Federal de Transparencia y Acceso a la Información Pública, Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y Ley General de Transparencia y Acceso a la Información Pública.
[15] Ley núm. 29733/2011.
[16] Ley núm. 8968.
[17] Ley núm. 787/2012.
[18] Ley núm. 1266/2008 y Ley Estatutaria 1581/2012.
[19] Ley núm. 81/2019 sobre Protección de Datos Personales.
[20] Ley núm. 13709.
[21] Ley Orgánica de Protección de Datos Personales.
[22] Artículo 55 de la Ley General de Protección de Datos Personales, modificada por la Ley núm. 13.853/2019.
[23] Ley núm. 6534/2020.
[24] Artículo 31 de la Ley núm. 18331, de agosto de 2008.
[25] Artículo 19 de Ley Estatutaria 1581/2011.
[26] Decreto núm. 899/2017.

tanto, se les declara como países adecuados conforme el artículo 25, párrafo 6, de la Directiva 95/46/CE del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Ingresar en este sistema internacional de reconocimiento de un tratamiento adecuado a los datos personales tiene implicaciones trascendentales, pues permite el libre intercambio de datos entre los países involucrados y, por consiguiente, una facilitación importante para los servicios de comercio electrónico en entornos de confianza y seguridad.

50. En Iberoamérica, dos países poseen dicho estatus jurídico: la Argentina (desde el 2 de julio de 2003) (Decisión 2003/490/CE) y el Uruguay (desde el 12 de octubre de 2012) (Decisión de Ejecución 2012/484/UE). Ambas decisiones del Grupo de Trabajo creado por el artículo 29 de la Directiva 95/46/CE, que declaran la adecuación de la Argentina y el Uruguay, destacan que se realizará un seguimiento de la evolución de la protección de datos y la forma como las respectivas autoridades de protección de datos aplican los principios de protección de datos que el sistema europeo propugna. Es de interés destacar que, en 2016, tanto la Decisión 2003/490/CE de la Comisión como la Decisión de Ejecución 2012/484/UE, entre otras relativas a la protección adecuada de los datos personales por varios países en aplicación del artículo 25, párrafo 6, de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sufrieron una modificación, que fuera aprobada por Decisión de Ejecución (UE) 2016/2296 de la Comisión, de 16 de diciembre de 2016, que se funda en el hecho de que el nivel de protección que los terceros países han garantizado puede estar sujeto a cambios y en que le corresponde a la Comisión comprobar periódicamente si la conclusión relativa a la adecuación del nivel de protección por el tercer país en cuestión está objetiva y jurídicamente justificada.

51. Cabe mencionar que la Argentina, en el año 2000, fue el primer país de América del Sur en aprobar una ley conforme al modelo europeo de protección de datos personales. La Ley núm. 25.326 comprende la protección de datos personales asentados en archivos, registros, bancos de datos y otros medios técnicos de tratamiento de datos, públicos o privados, tanto de personas físicas como jurídicas, en lo pertinente.

52. La Ley prevé una acción de *habeas data* a nivel constitucional en lo referente a datos personales a efectos de que el titular tenga acceso a sus datos y pueda requerir la rectificación o eliminación de datos inexactos o usados para un propósito discriminatorio.

53. Los principios generales relativos a la protección de datos previstos en la Ley son: licitud, finalidad, calidad de los datos, consentimiento, proporcionalidad, información, categoría de los datos, reconocimiento de los datos sensibles y principio de seguridad de los datos.

54. El sistema argentino consagra asimismo los derechos de acceso, rectificación y cancelación, así como el derecho de información para el caso de bases de datos públicas.

55. El Uruguay, por su parte, fue el siguiente en seguir el modelo del sistema enunciado cuando en agosto de 2008 aprobó una ley general (Ley núm. 18331) que rige para datos registrados en cualquier clase de soporte, tanto si se encuentran en dominios públicos como privados, y así se trate de personas físicas o jurídicas, con algunas excepciones.

56. Los principios que informan el sistema uruguayo de protección de datos son: el principio del consentimiento como base legitimadora del tratamiento del dato; el principio de limitación por razón de la finalidad; el principio de legalidad, calidad y proporcionalidad; el principio de transparencia; y el principio de seguridad. Los principios de buena fe, responsabilidad y minimización también son acordes con lo preceptuado legalmente.

57. El sistema uruguayo de protección de datos consagra, asimismo, los derechos de acceso, rectificación, actualización, inclusión o supresión a favor de los titulares de los datos, siempre que se den los requisitos establecidos en la norma, en conformidad con el sistema europeo de protección de datos.

58. El registro de las bases de datos es de carácter obligatorio. En este sentido, la ley uruguaya sigue los lineamientos de disposiciones normativas que han ido quedando obsoletas. En su lugar, esas disposiciones que reglamentaban la obligatoriedad del registro dejaron paso a sistemas de responsabilidad proactiva.

59. La ley reglamenta tanto acciones de carácter administrativo como una acción judicial expedita que podrá ser entablada por el titular de los datos.

60. Esta forma de encauzar los asuntos relativos a la protección de datos de carácter personal tuvo sus repercusiones en Iberoamérica, en tanto en cuanto siguieron aprobándose leyes con características similares a las del sistema europeo en otros países. Así sucedió entre 2010 y 2013 en Colombia, Costa Rica, México, Nicaragua y el Perú. Ya en aquel entonces se vislumbraba la constitución de un sistema iberoamericano de protección de datos como un modelo a seguir.

61. Iberoamérica no solo iba conformando su sistema de protección de datos personales, sino que también iba construyendo un modelo de armonización y cooperación que trascendía hacia la Unión Europea y procuraba mejorar el flujo de las economías, además de proteger el derecho humano fundamental a la privacidad y a la protección de los datos personales.

V. El sistema iberoamericano: estado actual

62. El Reglamento General de Protección de Datos de la Unión Europea (UE) 2016/679, que fue adoptado en 2016 y entró en vigor en 2018, tuvo un gran impacto en el mundo entero y también en Iberoamérica.

63. Algunas de las modificaciones que impuso el Reglamento son: la instauración de un sistema de protección del dato con un sistema de responsabilidad de carácter más proactivo que elimina la obligatoriedad del registro, la implementación de los procedimientos de privacidad por diseño y por defecto, la regulación de las evaluaciones de impacto, la reglamentación del derecho a la portabilidad de los datos, la obligatoriedad de las denuncias ante quiebres en los sistemas de seguridad y la dotación al sistema de sanciones más severas para casos de incumplimiento, entre otras.

64. Si bien Iberoamérica va conformando su ordenamiento en la dirección del Reglamento General de Protección de Datos de la Unión Europea, ninguna legislación ha incorporado las normas europeas en forma plena, y son pocos los países latinoamericanos que han aprobado disposiciones en concordancia con las innovaciones del Reglamento.

65. No obstante, las leyes de protección de datos aprobadas con posterioridad a la vigencia del Reglamento (2018) siguen su lineamiento general y se van posicionando en sintonía con el actual sistema de la Unión Europea. Tal es el caso del Brasil (2018), Panamá (2019), Andorra (2021) y el Ecuador (2021). Otros ordenamientos positivos iberoamericanos van adaptándose gradualmente a sus disposiciones.

66. En tal sentido, el Ecuador aprobó la Ley núm. 459, Orgánica de Protección de Datos Personales el 26 de mayo de 2021, que sigue los principios del Reglamento General de Protección de Datos de la Unión Europea, en especial en lo que concierne a sus lineamientos garantistas; los derechos de acceso, rectificación, cancelación y oposición; el derecho a la portabilidad y el principio de responsabilidad proactiva.

67. Panamá, por su parte, aprobó la Ley núm. 81 el 26 de marzo de 2019, que entró en vigencia en marzo de 2021. Su decreto de ejecución es de mayo de 2021. Entre otras innovaciones, la Ley prevé el principio de portabilidad.

68. Otros países, como es el caso del Uruguay, armonizaron sus disposiciones con las del Reglamento General de Protección de Datos de la Unión Europea previendo la figura del delegado de protección de datos, que en determinados casos es de creación obligatoria y tiene por función asesorar en la formulación de medidas de protección de datos, supervisar su cumplimiento, proponer nuevas medidas y actuar como nexo con la autoridad de control. También se estableció la obligación de realizar análisis del impacto del tratamiento de los datos personales cuando se dan las condiciones legales al efecto. El principio de seguridad se vio actualizado por la Ley núm. 19.670 y el Decreto núm. 64/2020, que se afilian también a las normas del Reglamento consagrando los principios de responsabilidad proactiva y privacidad por diseño y por defecto.

69. En el mismo sentido, Costa Rica tiene en consideración el proyecto de ley núm. 22388, que constituye una enmienda integral a la Ley de Protección de la Persona frente al

Tratamiento de sus Datos Personales (Ley núm. 8968). En el proyecto de ley se regula la figura del delegado de protección de datos, se consagra la necesidad de realizar evaluaciones de impacto en materia de privacidad, se modifican las disposiciones relativas al registro de bases de datos, se regula el consentimiento de los menores de edad y se incluyen disposiciones sobre privacidad por consideraciones similares a las del Reglamento General de Protección de Datos de la Unión Europea.

70. Se analizan a continuación algunos elementos que hacen que algunos sistemas de protección de datos y privacidad tengan un grado mayor de exigencia, como es el caso del europeo, y su incorporación en la legislación iberoamericana.

71. En lo que hace al delegado de protección de datos, el Ecuador lo regula en el artículo 85 de su Ley Orgánica de Protección de Datos Personales, recientemente aprobada. En el caso del Brasil, también está especialmente considerada la figura del delegado de protección de datos en el artículo 23 de la Ley General de Protección de Datos. El Uruguay regula minuciosamente esta figura en el artículo 40 de la Ley núm. 19.670 y en el Decreto núm. 64/2020. En México, el oficial de protección de datos personales es objeto de regulación en el artículo 85 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, y Colombia considera esta figura en el artículo 23 del Decreto núm. 1377/2013.

72. En lo que refiere a vulneraciones de seguridad, el Ecuador las tiene en consideración en el artículo 79 de su Ley Orgánica de Protección de Datos Personales, el Brasil en el artículo 48 de su Ley General de Protección de Datos, el Uruguay en el capítulo II del Decreto núm. 64/2020 y México en el artículos 38 y siguientes de su Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. La Argentina no tiene regulación al respecto, aunque ha aprobado una serie de recomendaciones sobre seguridad de la información, sin carácter de obligatoriedad[27]. En Costa Rica las vulneraciones de seguridad están reguladas en el artículo 38 del Reglamento a la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales. En Colombia la Ley Estatutaria 1581/2012 las considera en su artículo 17 y Panamá en el artículo 2, párrafo 5, de la Ley núm. 81, de marzo de 2019. Nicaragua, en el artículo 11 de su Ley núm. 787/2012, establece una comunicación obligatoria al Ejército o a la Policía Nacional. Las normas determinan la obligatoriedad de la comunicación a la autoridad de protección de datos y/o al titular del dato personal que ha sido objeto de un incidente de seguridad, y en algunos casos se determinan plazos específicos al efecto.

73. En cuanto a las evaluaciones de impacto en materia de protección de datos personales, el Brasil las tiene consagradas en su Ley General de Protección de Datos[28], México las tiene consagradas desde 2017[29] con carácter obligatorio para determinados casos especialmente establecidos. En el Uruguay[30] tienen carácter obligatorio solo cuando la ley así lo establece y en el Ecuador están consagradas en su Ley Orgánica de Protección de Datos Personales de 2021[31]. En la Argentina, Colombia, Costa Rica y la República Dominicana las evaluaciones de impacto no tienen carácter obligatorio.

74. El derecho a la portabilidad es otra de las modificaciones que impone el Reglamento General de Protección de Datos de la Unión Europea. En tal sentido, siguiendo su orientación, el derecho a la portabilidad está consagrado en la reciente Ley Orgánica de Protección de Datos Personales del Ecuador en tanto en cuanto establece lo siguiente: “El titular tiene el derecho a recibir del responsable del tratamiento sus datos personales en un formato compatible, actualizado, estructurado, común, interoperable y de lectura mecánica, preservando sus características; o a transmitirlos a otros responsables” [32]. Panamá también lo tiene consagrado[33]. Asimismo, el Brasil tiene el derecho a la portabilidad consagrado en su

[27] Resolución núm. 47/2018.
[28] Artículo 10, numeral 3.
[29] Artículo 74 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
[30] Artículo 6 del Decreto núm. 64/2020.
[31] Artículo 42.
[32] Artículo 17.
[33] Artículo 15, párrafo 5, de la Ley núm. 81/2019.

Ley General de Protección de Datos[34], al igual que Chile[35]. El Salvador[36], Honduras[37] y el Uruguay[38] regulan específicamente la portabilidad numérica. En el Paraguay[39] el derecho a la portabilidad se encuentra protegido únicamente para datos crediticios.

75. De esta forma se produce un avance más en el sistema, dado que no solo se sigue el modelo tradicional europeo, sino que también en Iberoamérica se trabaja en pos de actualizar las normas a su semejanza, procurando mejorar los medios de cooperación entre Iberoamérica y la Unión Europea.

VI. Conclusiones

76. **Los derechos de las personas siempre deben conducir a realzar la dignidad y la autonomía, la igualdad y la libertad de la persona humana, así como a coadyuvar en su convivencia social y política, en tanto en cuanto la persona es el origen y el fin de toda organización jurídica y política.**

77. **Aun a falta de una disposición que expresamente regule los temas de privacidad, protección de datos personales y *habeas data*, el amparo al derecho humano fundamental se encuentra presente y tiene por fundamento una concepción iusnaturalista que impregnó las constituciones iberoamericanas hasta finales del siglo pasado.**

78. **Tres hitos marcaron la evolución del sistema iberoamericano de protección de datos personales. El primero es la Declaración de la XIII Cumbre Iberoamericana de Jefes de Estado y de Gobierno de Santa Cruz de la Sierra, de noviembre de 2003. El segundo es la Declaración de La Antigua, de junio de 2003. El tercero es la Declaración de Cartagena de Indias, de 2004.**

79. **La mayor parte de los países iberoamericanos consideran en sus constituciones el derecho a la privacidad un derecho humano fundamental.**

80. **La protección de datos personales es también un derecho humano fundamental, aunque no se encuentra explícitamente consagrado constitucionalmente. Ahora bien, durante los primeros tres lustros del siglo XXI, la tendencia de los países iberoamericanos ha ido hacia la promulgación de leyes que se basan en el sistema europeo de protección de datos personales, complementándose así las disposiciones programáticas de las respectivas constituciones de los países de Iberoamérica.**

81. **Es característica del sistema la existencia de una ley general en la materia que abarca en forma integral los datos personales.**

82. **En dicha ley se establecen una serie de principios que habrán de ser honrados y respetados. Se incluyen obligaciones, derechos y responsabilidades de los distintos sujetos en juego. Se regula asimismo la creación de una autoridad de control en datos personales de carácter autónomo que puede ejercer sus actividades en forma preventiva y también a posteriori sancionando los incumplimientos. Es importante que posea instrumentos jurídicos para hacer valer en forma administrativa y judicial los distintos derechos en juego.**

83. **Del análisis de estos principios en la realidad normativa iberoamericana se concluye la existencia de un sistema de protección de datos personales que actúa cual modelo de armonización y cooperación, trascendiendo hacia la Unión Europea, procurando el sano equilibrio entre la protección del derecho humano fundamental y**

[34] Artículo 18 (V), según redacción modificada por la Ley núm. 13.853/2019.
[35] Artículo 9 de la Ley núm. 19.628, de 18 de agosto de 1999, modificada en 2018.
[36] Artículo 19 e) del Decreto legislativo núm. 142 de Telecomunicaciones y Energía, de 6 de noviembre de 1997, reformado en 2008.
[37] Ley de Portabilidad Numérica, de 30 de abril de 2014.
[38] Artículo 471 de la Ley núm. 19889, de 9 de julio de 2020.
[39] Artículo 8º de la Ley 6534/2020 de Protección de Datos Personales Crediticios.

la libre circulación de mercancías, personas, servicios y capitales, y propendiendo a su vez a una sana integración económica y social.

84. **La aprobación y entrada en vigencia del Reglamento General de Protección de Datos de la Unión Europea (UE) 2016/679 tuvieron fuertes repercusiones en Iberoamérica, que ha ido adoptando las distintas soluciones que el Reglamento propone sobre cuestiones como la necesidad de tener una persona responsable de la protección de datos en cada organismo, la forma de comunicación y tramitación de los incidentes de seguridad, las medidas de responsabilidad proactiva, la evaluación de los potenciales riesgos en las distintas etapas del ciclo vital del dato y el derecho de portabilidad, entre otras.**

85. **Partiendo del entendimiento de que la cooperación es un elemento de la esencia de la protección de datos personales, el sistema iberoamericano de protección de datos procura armonizar sus normas conforme al modelo europeo a efectos de lograr un mayor nivel de integración en la materia con Europa.**

86. **Si bien del análisis realizado se desprende que no todas las disposiciones e institutos de la protección de datos se encuentran considerados en las distintas legislaciones de Iberoamérica, surge claramente de los ejemplos mencionados la existencia de una tendencia a la protección integral de la privacidad y los datos personales cada vez más marcada, con netas influencias europeas, que constituye el sistema iberoamericano de protección de datos personales.**

VII. Prospectiva

87. De lo expuesto surge la existencia de un sistema de protección de datos personales hacia el que propende Iberoamérica que se conforma en base a los principios europeos en materia de protección de datos personales. Se percibe de ese modo una forma de estructurar un interesante mecanismo de cooperación entre Iberoamérica y Europa que viene desarrollándose desde hace dos décadas en un ámbito geográfico cada vez mayor dentro del continente americano.

88. Esta forma de trabajo bien puede considerarse un ejemplo para contribuir al desarrollo de los principios de privacidad y protección de datos en el contexto global, siempre que esta integración logre realizarse armónicamente en base a respetos recíprocos, con menos discriminación y más justicia, y en un mundo en el que rijan los principios democráticos y el desarrollo económico de los pueblos se vea favorecido en tanto en cuanto solo partiendo de una concepción integrada de los principios se pueden encauzar pilares tecnológicos disruptivos en materia de privacidad como los que plantean las tecnologías de inteligencia artificial, realidad virtual, biotecnología, Internet de las cosas y videovigilancia masiva.

89. Los desafíos son alcanzables, y la integración y la armonización habrán de constituirse en nuestras metas, siempre teniendo en mente ayudar a los grupos especialmente desfavorecidos conforme a parámetros éticos y respetando las diversidades.