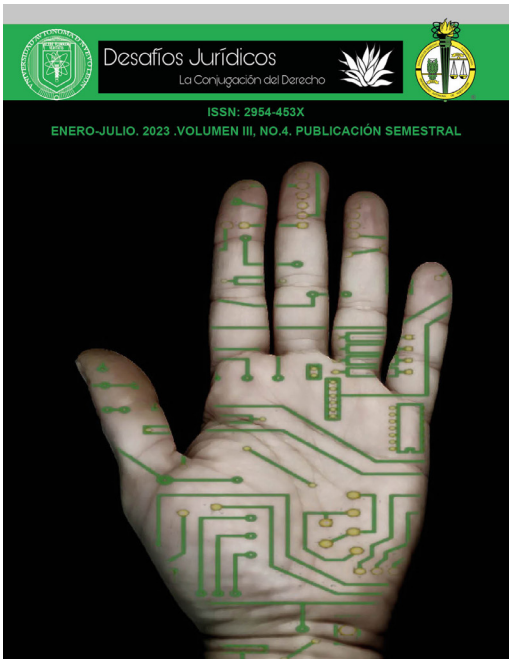

Detalles sobre la publicación, incluyendo instrucciones para autores e información para los usuarios en: https://desafiosjuridicos.uanl.mx/index.php/ds

Yarina Amoroso (Universidad de Ciencias Informáticas) y **Jacqueline Guerrero** (Universidad Internacional del Ecuador)

El panorama legislativo de la protección de datos en Latinoamérica en el período 2018-2022. pp. 50-77. Fecha de publicación en línea: 31 de enero del 2023.

Desafíos Jurídicos Vol. 3 Núm. 4, Enero-Junio 2022, es una publicación semestral editada por la Universidad Autónoma de Nuevo León, a través de la Facultad de Derecho y Criminología. Dirección de la publicación: Av. Universidad s/n Cd. Universitaria C.P. 66451, San Nicolás de los Garza, Nuevo León, México. desafiosjuridicos.uanl.mx,-desafiosjuridicos@uanl.mx. Editora responsable: Dra. Amalia Guillén Gaytán, Facultad de Derecho y Criminología. Reserva de Derechos al Uso Exclusivo núm. 04-2022-041510211500-102. ISSN 2954-453X, ambos otorgados por el Instituto Nacional del Derecho de Autor. Responsable de la última actualización: Dr. Paris Alejandro Cabello Tijerina, Facultad de Derecho y Criminología, Av. Universidad s/n, Cd. Universitaria, C.P., 66451, San Nicolás de los Garza, Nuevo León, México.

El panorama legislativo de la protección de datos en Latinoamérica en el período 2018-2022[a]

The legislative panorama of data protection in Latin America in the period 2018-2022

Fecha de publicación en línea: 31 de enero del 2023

Por: Yarina Amorosos* y Jacqueline Guerrero**

* https://orcid.org/0000-0002-0185-082X
Universidad de Ciencias Informáticas
** https://orcid.org/0000-0002-3513-8291
Universidad Internacional del Ecuador

Resumen. La protección de datos personales ha tenido un desarrollo legislativo a nivel mundial, con características acorde a la realidad de cada país o región, permitiendo establecer modelos de regulación con diferentes enfoques. América Latina, en los últimos veinte años, ha sido influenciada por la tradición europea continental. Sin embargo, eran pocos los países latinoamericanos que tenían normativa específica de protección de datos antes de la vigencia del Reglamento de la Unión Europea 2016/679, emanado del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (RGPD); y, únicamente cuatro han aprobado leyes sobre la materia posterior a la vigencia de la referida norma.

El artículo explica la correspondencia del marco normativo relativo a la protección de datos de algunos países latinoamericanos con los estándares más importantes del Reglamento de la Unión Europea 2016/679 emanado del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de los mismos. Para este efecto, se realiza un análisis comparativo que permita determinar el contenido y alcance de categorías específicas de las propuestas legislativas de los países latinoamericanos que cuentan con normativa específica de protección de datos vigentes posterior al 2018, a fin de identificar los rasgos particulares.

Palabras clave: protección de datos personales; intimidad; privacidad.

a Este trabajo se desprende del proyecto de investigación Lex Infodata: panorama de la protección de datos en Latinoamérica, desarrollado conjuntamente por la Mgt. Yarina Amoroso, de la Universidad de Ciencias Informáticas de Cuba; Dra. Nayibe Chacón, de la Universidad Central de Venezuela, Dra. Myrna García, de la Universidad de Nuevo León de México; Dra. Jacqueline Guerrero, de la Universidad Internacional de Ecuador; Dra. Laura Nahabetián, de la Universidad Mayor de la República Oriental del Uruguay; y, Dra. Patricia Reyes, de la Universidad de Valparaíso, Chile.

Abstract. The data protection has had a worldwide legislative development, with characteristics according to the reality of each country or region, allowing the establishment of regulatory models with different approaches. Latin America, in the last twenty years, has been influenced by the continental European tradition. However, few Latin American countries had specific data protection regulations before the validity of the European Union Regulation 2016/679, issued by the European Parliament and the Council, of April 27, 2016 (GDPR); and only four have approved laws on the matter after the entry into force of the aforementioned regulation.

The article explains the correspondence of the regulatory framework relating to data protection in some Latin American countries with the European Union Regulation 2016/679 issued by the European Parliament and the Council of April 27, 2016, relative to the protection of natural persons with regard to the processing of personal data and their free circulation. For this purpose, a comparative analysis is carried out to determine the content and scope of specific categories of the legislative proposals of Latin American countries that have specific data protection regulations in force after 2018, in order to identify the particular features.

Key words: personal data protection; privacy; privacy.

INTRODUCCIÓN

En el contexto de las sociedades actuales se hace cada vez más habitual el uso de las computadoras y el acceso a Internet, lo cual ha ocasionado una significativa transformación en todos los procesos y ha generado un nuevo orden social caracterizado por la importancia de la información. El advenimiento y expansión de Internet, como la red de redes que vincula a millones de individuos en todo el mundo, ha trascendido en la concentración, sistematización y disponibilidad de información personal para diferentes fines. Se enfrentan, además, otros desafíos provenientes de una tecnología en constante avance, tal es el caso del Big Data, la Internet de las cosas, la computación en nube y la inteligencia artificial. Sin embargo, estos adelantos tecnológicos forman parte de la realidad más rápidamente que las respuestas jurídicas dadas a los problemas por ellos originados.

Con el objetivo de atenuar las problemáticas que el desarrollo tecnológico provoca para el desenvolvimiento de la persona humana, así como para la propia sociedad, se han promulgado un grupo de normativas cuyo fin ha sido la protección de los datos personales, a partir de las Constituciones, como norma suprema que ordena los principios básicos para este derecho. También se han adoptado estándares para la región iberoamericana donde se plantean nuevos retos a los ordenamientos jurídicos. Estos constituyen una convocatoria para la actualización de las legislaciones vigentes, con base en las mejores prácticas, así como un incentivo para aquellos países que aún no cuentan con legislaciones específicas.

El propósito es que se legisle sobre el particular, pues el uso de las TIC y las redes sociales, en particular, convierten a este asunto en un tema que acompaña a todos los individuos en su andar por el Ciberespacio, desde cualquier lugar en que se acceda o se realice el tratamiento de los datos personales.

Teniendo en cuenta las disímiles normativas que se han aprobado desde la década de los 70 del siglo XX, en la que se evidencian las primeras manifestaciones del derecho a la protección de los datos personales, se pueden identificar algunos rasgos que distinguen a dichas regulaciones (Ojeda Bello 2020). En tal sentido se aprecia cómo los criterios de regulación son diferentes de acuerdo con el contexto, en unos casos con sistemas integrales de protección y en otros a través de normas generales, no específicas y sectoriales. Además, se delimitan las garantías de los derechos individuales a partir de establecer límites al empleo de la informática y regular el derecho de acceso de las personas a las informaciones que les conciernen.

Así mismo, se aprecia un mayor desarrollo normativo en Europa, no así en Latinoamérica donde se evidencia un retardo, tanto en el orden constitucional como legislativo. Sin embargo, solo hasta finales de la década de los 90 es que se logra definir estándares de protección que permitieron el flujo de datos entre los Estados Unidos de Norteamérica y Europa. En el contexto latinoamericano, los textos constitucionales reconocen, en su mayoría, el derecho a la protección de datos personales asociado al derecho a la intimidad y su regulación la expresan en ocasiones en forma de garantía específica o como un tipo de acción de amparo; y, por último, la definición del carácter autónomo e independiente del derecho con rango constitucional no siempre se equipara con la aprobación de una ley específica que amplíe los preceptos de la Ley Suprema, lo cual implica un desarrollo jurisprudencial notable.

De esta forma en los diferentes países donde se ha regulado, constitucionalmente o en una ley específica, se expresan características distintivas en los que el desarrollo tecnológico, las problemáticas asociadas y otros factores políticos han incidido en las disímiles formas en las que se fuera configurando, cada vez con una mayor autonomía, el derecho a la protección de datos personales (Ojeda Bella, Zahira y Yarina Amoroso 2016)

VALORACIONES TÉCNICO CONCEPTUALES DEL DERECHO A LA PROTECCIÓN DE DATOS

Desde la década de los 70 del siglo XX, progresivamente, se supera el concepto restringido de derecho a la intimidad. Éste, aplicado a los avances tecnológicos actuales, da paso a la denominación de derecho a la autodeterminación informativa o libertad informática y años más tarde emerge como un derecho autónomo e independiente denominado derecho a la protección de datos personales.

La diversidad de criterios expuestos en estos últimos años, con independencia de los elementos que cada uno de ellos tuvo en cuenta para ofrecer una conceptualización del derecho a la protección de datos personales, ha permitido determinar que debe ser entendido como aquel a través del cual se aseguran to-

dos aquellos datos de carácter personal, que identifiquen o sean susceptible de identificación y a tal efecto le ocasionen alguna afectación al titular de los mismos. En consecuencia, el titular podrá solicitar el acceso, la rectificación, cancelación u oponerse al tratamiento y uso de sus datos. De ahí que la intensificación de los riesgos que la compilación y sistematización de los datos de carácter personal ha provocado, con el auge creciente de las tecnologías de la información y las comunicaciones, ha permitido clarificar las diferencias entre lo reconocido como derecho a la intimidad, el derecho a la autodeterminación informativa o libertad informática y el derecho a la protección de datos personales.

La ordenación de las sociedades del siglo XXI debe ser vista desde el desarrollo tecnológico alcanzado, unido a las formas de estudio y regulación en el ámbito jurídico de las problemáticas sobrevenidas. Al decir de Delpiazzo "(…) para que el cambio tecnológico sea sumido y no sufrido por la sociedad, se requiere que el derecho se adecue a la nueva realidad emergente" (2003, 55). Frente a este panorama los individuos se encuentran a merced de un sinnúmero de situaciones que alteran sus derechos humanos, que a decir de la Dra. C. Danelia Cutié Mustelier se entienden como:

> aquellas exigencias y facultades inherentes a la dignidad humana reconocidas por el ordenamiento jurídico nacional en correspondencia con el desarrollo histórico y a tono con los documentos aprobados por la Comunidad Internacional, que requieren de una determinada condicionalidad material, que permita su viabilidad social y de un férreo sistema de garantías que de forma integral proporcione una rápida y eficaz tutela de los mismos, ante cualquier acto o actuación proveniente de agentes o funcionarios estatales, así como de particulares que los amenacen o vulneren", y no la de derechos fundamentales por cuanto esta última se refiere a "una jerarquización protectora utilizando la vía judicial para la defensa de dichos derechos, más que enfocarlos como naturales, mientras que el término derechos humanos permite defender la postura de que todos los derechos son iguales, interdependientes e indivisibles y por tanto imprescindibles para la vida humana y de esta forma pueden situarse al mismo nivel, dotarlos de iguales garantías y ofrecerles la misma protección (Cutié 1999, 30).

La comprensión del derecho a la protección de datos personales como un derecho autónomo se enmarca en el análisis de las generaciones de derechos y como parte del proceso de evolución histórica de los derechos humanos, que para autores como García González (2007, 746) constituyen categorías históricas determinadas que tienen sentido en contextos temporales específicos (García 2007). Con base a ello, aunque la identificación de tres generaciones[1] de derechos (Villabella 2020,

1 Con fines metodológicos y para indicar el iter evolutivo de los derechos, sin querer establecer jerarquizaciones que indiquen distinciones entre los mismos, se hace referencia a las generaciones de derechos. La primera de ellas, pertenece a las Revoluciones Liberales del siglo XVIII en la que se marcaron los derechos individuales de defensa de la persona, cuya exigencia consistió en la autolimitación y la no injerencia de los poderes públicos en la esfera íntima de la persona. Se

146-148) es la postura más común entre los estudiosos, se identifica por Bustamante (2010, 10) una cuarta generación[2] ubicada en lo que se ha denominado por Castell (2002, 50) como sociedad de la información y del conocimiento,[3] teniendo en cuenta el referido impacto causado por la aparición y desarrollo universal de las tecnologías de la información y las comunicaciones. Tanto los beneficios como las contradicciones manifiestas para su uso y explotación, han llevado a una nueva comprensión de los derechos humanos, en tanto la influencia de la tecnología informática dota de un significado diferente a un grupo de principios éticos que exige contar con un modelo jurídico adecuado.

Al referirse al innegable proceso evolutivo que sufren los derechos Pérez Luño afirma:

> (…) el cambio de generación es esencial y expresa por tanto que el papel de los derechos fundamentales deja de ser el mero límite a la actuación estatal para transformarse en instrumentos jurídicos de control de su actividad positiva, que debe estar orientada a posibilitar la participación de los individuos y los grupos en el ejercicio del poder. Lo que trae como consecuencia la necesidad de incluir en el sistema de los derechos fundamentales no solo a las libertades clásicas, sino también a otros como categorías accionables y no como meros postulados programáticos (Pérez Luño 1991, 228).

Todo lo cual lleva a que el derecho constitucional en el presente siglo, desarrolle procesos de positivización de nuevas categorías de derechos humanos así como la adecuación de las ya existentes, teniendo en cuenta el entorno de la sociedad de la información y el conocimiento. En consecuencia, el adveni-

reconocen, por ejemplo, el derecho al honor, el derecho a la intimidad, el derecho a la vida y a la integridad personal. La segunda generación se ubica desde las luchas sociales del siglo XIX y hasta el siglo XX con la formulación de la Declaración Universal de los Derechos Humanos 1948. Caracterizada por la intervención del Estado para garantizar los derechos de carácter económico y social. Surgen derechos como: a la seguridad social, a la educación, a la salud y al trabajo. La tercera generación, se ubica a partir de la segunda mitad del siglo XX. El promotor de estos derechos será la acción de determinados colectivos que reclaman sus legítimos derechos. Se configuran derechos en forma de declaraciones sectoriales que protegen derechos de sectores excluidos o minorías étnicas o religiosas afectados por las múltiples manifestaciones de la discriminación económico-social. Se destacan derechos como la autodeterminación, el medio ambiente, la identidad nacional y cultural. La solidaridad caracteriza a estos nuevos derechos ya que ellos se hallan aunados entre sí por su incidencia mundial en la vida de todos los seres humanos y exigen para su realización la comunidad de esfuerzos y responsabilidades a escala universal.

2 Debe ser entendida como una forma de garantizar el nuevo status del individuo de la sociedad digital (su personalidad virtual) provocado por la universalización del acceso a las tecnologías de la informática y las comunicaciones, la libertad de expresión en la red y la libre distribución de la información y el conocimiento.

3 El término “sociedad del conocimiento” se ha confundido o utilizado como sinónimo de “sociedad de la información”. La información se compone de hechos y sucesos, mientras que el conocimiento se define como la interpretación de dichos hechos dentro de un contexto, con alguna finalidad. Ello implica reconocer que la sociedad de la información es la base de la sociedad del conocimiento, en tanto esta última se refiere a la apropiación crítica y selectiva de la información para producir conocimiento.

miento de la cuarta generación de los derechos humanos garantizará el nuevo status del individuo de la sociedad digital. Lo anterior, no impide afirmar que a partir de la tercera generación de derechos se hace más evidente la adecuación de las instituciones jurídicas, así como su normatividad, en defensa de la persona, en tanto se dota de protección o se intensifican las ya existentes, a esas nuevas categorías de derechos que no habían sido con claridad identificadas.

Justo en la década del 70 del siglo XX, comienza a construirse el perfil del llamado derecho a la autodeterminación informativa,[4] que se identifica como un nuevo derecho y considera que el concepto de derecho a la intimidad se limita al ámbito más próximo de la persona, es decir el de los datos revelados a un círculo de relaciones restringidas y sin extenderse a los datos protegidos en materia informática; contenido incluido en el derecho a la autodeterminación informativa, de ahí su ubicación por separado (Amoroso 2019).

Pérez Luño (1994, 12) lo refiere también, como un nuevo derecho fundamental denominado de libertad informática propio de la tercera generación, cuya finalidad es asegurar la facultad de las personas de conocer y acceder a las informaciones que les conciernen archivadas en bancos de datos, así como controlar su calidad. Hecho que implica la posibilidad de corregir o cancelar los datos inexactos o indebidamente procesados y disponer sobre su transmisión. Por su parte Puccinelli (1999, 4) sostiene que el concepto de libertad informática ofrece un contenido erróneo en relación a la protección de los datos de carácter personal y resalta la proyección del principio–valor libertad que desde su visión, aplicado a la actividad informática, se traduce en el derecho de los operadores de dichos sistemas de colectar, procesar y transmitir toda la información, cuyo conocimiento, registro o difusión no esté restringido desde lo legal por motivos razonables, fundados en la protección de los derechos de las personas o en algún interés colectivo relevante que justifique tal limitación.
Sin dejar de tener en cuenta el proceso de desarrollo del derecho objeto de estudio, en tanto se concibió en sus primeras formas de manifestación como parte del derecho a la intimidad, lo analizado hasta aquí, evidencia cómo en ocasiones se incluyen los datos personales de manera desacertada dentro del ámbito de salvaguarda del derecho a la intimidad,[5] sin declararse aún su carácter autónomo e independiente.

A tal efecto tras el precedente análisis teórico – conceptual, se aprecia cómo la definición del derecho se hace desde diversos posicionamientos teóricos, en unos casos desde el derecho a la intimidad y en otros como autodeterminación informativa o libertad informática e incluso se manifiestan diversas posturas en cuanto a si es un derecho o una garantía. Además al enunciarse problemáticas ocasionadas por el avance de las tecnologías de la informa-

4 Adquiere rango constitucional a partir de la sentencia del 15/12/1983, del Tribunal Constitucional Federal alemán, donde se presenta recurso contra la Ley de 25/3/1982, sobre el censo demográfico, al excederse en la solicitud de información que se solicitaba a los ciudadanos.

5 La primera enunciación del derecho a la intimidad se encuentra en 1890, en los Estados Unidos de Norteamérica, con la obra The right of privacy de Samuel Denis Warren y Louis Denmbitz Brandies, como contrapartida a la extralimitación de la prensa en los asuntos íntimos de las personas.

ción se hace desde la vulneración del derecho a la intimidad; mientras que al definir el objeto de protección de este derecho se hace desde el enfoque de los datos informáticos.

En consecuencia el derecho a la protección de datos personales se identifica como autónomo e independiente al contar con un contenido, principios y garantías propias, aún cuando se relaciona y asegura otros derechos, de ahí su carácter instrumental. Se ubica en una cuarta generación de derechos humanos, teniendo en cuenta las novedosas formas de relaciones sociales expresadas tras el vertiginoso avance de las tecnologías de la información y las comunicaciones.

Con base en este breve análisis conceptual del derecho a la protección de datos, a continuación se describe la consagración del derecho a la protección de datos en las legislaciones de Brasil, Cuba, Panamá, Ecuador y Uruguay, que son los países que han aprobado normativa específica o reformado la existente, posterior a la vigencia del RGPD. Ello en razón de que la investigación es descriptiva y con enfoque cualitativo, pues interpreta a partir del contenido de las legislaciones de Brasil, Cuba, Panamá, Ecuador y Uruguay, los elementos comunes y las diferencias de ciertas categorías específicas.

LA SITUACIÓN DE LATINOAMÉRICA AL 2022

Marcos jurídicos nacionales

Brasil

Al igual que otros países latinoamericanos, el antecedente del derecho a la protección de datos en Brasil radica en el habeas data, previsto en la Constitución Política de la República Federativa de Brasil de 1988. La Carta constitucional consagra también, en su artículo 5 literal X, la inviolabilidad de la intimidad, la vida privada, el honor y la imagen de las personas.

Pese a que la Ley 13.709 de Protección de Datos, publicada el 14 de agosto de 2018, no es la primera norma relativa a la protección de datos en Brasil, brindó unidad legislativa a la materia en el país y es la primera ley de protección de datos en Latinoamérica aprobada posterior a la vigencia de RGPD, que evidencia una clara influencia europea, pues si bien no es una réplica del RGPD es consistente con los aspectos fundamentales. La Ley 13.709 se ha modificado dos veces[6], y está en pleno vigor desde el 15 de agosto de 2021.

La Ley General de Protección de Datos de Brasil contiene tres elementos decisivos: a) gobernanza de los datos; b) seguridad de la información; y, c) atención a los titulares de los datos. La gobernanza de los datos es uno de los pilares, que corresponde a las tareas de diagnóstico, evaluación de riesgos e impacto por la recolección, tenencia y uso de datos personales. El segundo pilar fundamental es la seguridad de la información que conlleva la gestión segura de los datos personales. Y, el tercer pilar corresponde a la definición de los servicios a los titulares de los datos persona-

6 La Ley 13.853 de diciembre de 2019 creó la Autoridad Nacional de Protección de Datos Personales, entidad adscrita al Ministerio de Justicia, que posteriormente se reglamenta mediante Decreto 10.474 de 26 de agosto de 2020; y, la Ley 14.010 de junio de 2020 pospuso la aplicación del régimen de sanciones, el cual está en vigor desde agosto de 2021.

les para asegurar el ejercicio de los derechos de los titulares de los datos (Baños 2019).

Cuba

En Cuba desde el año 2019 entró en vigor una nueva Constitución, en el Capítulo II Derechos, artículo 48, se dispone: "Todas las personas tienen derecho a que se les respete su intimidad personal y familiar, su propia imagen y voz, su honor e identidad personal".

En materia específica de protección datos derechos se correlacionan con lo dispuesto en el Capítulo VI Garantías de los derechos:

> "ARTÍCULO 97. Se reconoce el derecho de toda persona de acceder a sus datos personales en registros, archivos u otras bases de datos e información de carácter público, así como a interesar su no divulgación y obtener su debida corrección, rectificación, modificación, actualización o cancelación. El uso y tratamiento de estos datos se realiza de conformidad con lo establecido en la ley".

A partir de estos presupuestos el derecho inherente a la personalidad, conjuntamente con el derecho a la propia imagen y al honor se corresponde con el principio de la dignidad humana que reconoce a la persona en su lugar de privilegio, como individualidad que sustenta la formulación de todas las políticas públicas y desarrollos que se efectúan en la sociedad cubana.

Recientemente, el 14 de mayo de 2022, el parlamento cubano ha aprobado Ley de Protección de Datos Personales, en virtud del cual se protegen todas las informaciones cuya divulgación pueda impactar negativamente en la privacidad de las personas, dado que tal como se reconoce por la doctrina y la jurisprudencia internacional, el derecho de protección de datos alcanza a todo dato que bien identifique o permita identificar a una persona y conocer aspectos de su vida privada.

Se trata de elementos que integran el contenido esencial del derecho a la protección de datos personales y por tanto su vulneración ocasionará la violación a estas normas. Por otra parte, es a su vez fundamental, como hace la Ley, dejar establecido toda la secuencia de principios que informan al derecho de protección de datos personales, siendo más que una declaración de intenciones, pues son principios que se hacen efectivos a través del ejercicio de los derechos que los titulares de los datos tienen posibilitado.

Con la promulgación de la Ley de Protección de Datos, cambia para bien, el panorama alrededor de este sensible tema en el país. Se instalan las normas que viabilizan las garantías y derechos constitucionalmente reconocidos y se imponen desafíos para su ejercicio a favor de la consideración de la centralidad humanista que tiene por finalidad sostener el carácter de centro vital de las políticas públicas y las acciones individuales y colectivas con focalización en la persona como eje y base elemental de imputación de derechos, deberes, libertades y obligaciones. Para ello reclama de una reorganización institucional para su gestión efectiva, no solo para los datos en manos del sector público sino también el privado (Amoroso, 2022).

La Ley es portadora de una formulación propia de protección de datos personales, en vínculo

con las tecnologías presentes y emergentes. Es fundamental que la norma contenga un sistema de contravenciones, pero al mismo tiempo que haya sido aprobada al unísono de todo el conjunto de disposiciones procesales y el propio Código Penal, porque se crean las condiciones para evitar cualquier tipo de indefensión frente a un mundo tan tecnológicamente invasivo como el que comienza a ser parte con mayor intensidad en el día a día.

Unido a ello, además, y de manera intencionada se comienza a promover una cultura de respecto a la privacidad propia y ajena, advirtiendo sobre riesgos y medidas de protección a la ciudadanía.

Ecuador

La Constitución de la República del Ecuador, en vigencia desde el 20 de octubre de 2008, en su artículo 66, numeral 19, consagró el derecho a la protección de datos como un derecho de libertad, en términos de asegurar el acceso y la decisión sobre información y datos de carácter personal, sumándose de esta manera a los otros cuatro países latinoamericanos[7] que tienen el reconocimiento constitucional del derecho a la protección de datos como un derecho independiente del derecho a la privacidad e intimidad (OEA 2012). En este sentido, para la recolección, archivo, procesamiento, distribución o difusión de estos datos o información, la Constitución dispone que se requerirá la autorización del titular o el mandato de la ley.

A su vez, con la finalidad de proteger eficaz e inmediatamente el derecho a la protección de datos, declarar la violación del derecho y disponer la reparación integral del daño causado por la violación, en el Art. 82 de la Constitución se consagra la garantía jurisdiccional de Habeas Data, en los siguientes términos:

> Toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico. Asimismo tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos. Las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la ley. La persona titular de los datos podrá solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación. En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias. Si no se atendiera su solicitud, ésta podrá acudir a la jueza o juez. La persona afectada podrá demandar por los perjuicios ocasionados.

De conformidad con lo dispuesto en el artículo 50 de la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional, la Acción de Habeas Data se puede interponer en los

7 República Dominicana, Ecuador, Perú, México y Venezuela

siguientes casos: a. Cuando se niega el acceso a los documentos, datos genéticos, bancos o archivos de datos personales e informes que consten en entidades públicas o estén en poder de personas naturales o jurídicas privadas; b. Cuando se niega la solicitud de actualización, rectificación, eliminación o anulación de datos que fueren erróneos o afecten sus derechos; y, c. Cuando se da un uso de la información personal que viole un derecho constitucional, sin autorización expresa, salvo cuando exista orden de jueza o juez competente.

Ahora bien, en materia de protección de datos el Ecuador inaugura una nueva etapa con la vigencia de la Ley Orgánica de Protección de Datos, publicada en el quinto suplemento del Registro Oficial 459 de 26 de mayo de 2021. La norma tiene el carácter de orgánica, por lo cual prevalecerá sobre cualquier otra ley ordinaria, en razón de regular un derecho constitucional. La norma consta de doce capítulos y setenta y siete artículos.

La Ley Orgánica de Protección de Datos está en pleno vigor y conforme lo establece la Disposición General Séptima el ejercicio de los derechos reconocidos en la norma podrá ser exigido por el titular independientemente de la entrada en vigor del régimen sancionatorio. Sin embargo, la disposición transitoria segunda prevé una *vacatio legis* de dos años, a partir de la publicación de la Ley, para que los tratamientos de datos realizados en forma previa a la entrada en vigencia de la Ley se adecúen a lo previsto en la norma.

La ley ecuatoriana es la norma más actual, en cuanto a su aprobación posterior a la vigencia del RGPD, y, sigue el modelo europeo, con algunas modificaciones en virtud de que se trata de la primera ley en la materia que adopta el país y era necesaria una adecuación a la realidad propia y la escasa experiencia. Así, por ejemplo, Ecuador decidió no regular el tema del derecho al olvido, incluyó algunas categorías especiales de datos como los datos relativos a las discapacidades y mantuvo el sistema de registro de bases de datos, entre otros.

Panamá

Luego de Brasil, Panamá se convirtió en el segundo país en aprobar una ley de protección de datos posterior a la vigencia del RGPD. El 26 de marzo de 2019 Panamá publicó en su Gaceta Oficial la Ley 81 sobre Protección de Datos Personales, la cual entró en vigencia el 29 de marzo de 2021, y fue reglamentada mediante Decreto Ejecutivo 285 del 28 de mayo de 2021.

La Ley 81 encuentra fundamento de validez en el reconocimiento constitucional del derecho a la protección de datos, en el artículo 42 de la Constitución Nacional que señala:

> Toda persona tiene derecho a acceder a la información personal contenida en bases de datos o registros públicos y privados, y a requerir su rectificación y protección, así como su supresión, de conformidad con lo previsto en la Ley. Esta información solo podrá ser recogida para fines específicos, mediante consentimiento de su titular o por disposición de autoridad competente con fundamento en lo previsto en la Ley.

La Ley panameña, pese a ser una norma específica, no es la única que conforma el marco regulatorio de la protección de datos en Panamá. Esto debido a que existen otras norma aplicables como: la Ley Bancaria, Ley de Seguros, Ley de Valores, Ley fiduciaria, Ley que regula los derechos y obligaciones de los pacientes, en materia de información o decisión libre e informada (De la Guardia 2021).

Uruguay

Uruguay fue uno de los primeros países de Sudamérica en adoptar normativa de protección de datos orientada al cumplimiento de los estándares internacionales, así la Ley 18.331 del 11 de agosto de 2008 inauguró el marco normativo específico de la protección de datos. En la línea de concordancia con el RGPD, Uruguay aprueba importantes reformas a los artículos 37 al 40 de la Ley 18.331 a través de la Ley 19.670 de 15 de octubre de 2018.

La actualización del marco normativo de la protección de datos uruguayo se cierra con el Decreto No. 64/020 de 21 de febrero de 2020, que reglamenta la Ley 19.670 y con miras a lograr el nivel máximo de protección de datos la última reglamentación desarrolla temas fundamentales como: los casos de aplicación extraterritorial de la normativa de protección de datos; la obligación de notificar las vulneraciones de seguridad; la consagración del principio de responsabilidad proactiva; la obligación de contar con un delegado de protección de datos para ciertas entidades; y, la necesidad de establecer de manera escrita los servicios de tratamientos realizados por terceros (Castells 2020).

Se destaca que Uruguay adhirió al Convenio N° 108 del Consejo de Europa para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal y por la Ley 19.948 de 16 de abril de 2021 aprobó el Protocolo de enmienda del Convenio para la Protección de las Personas con respecto al Tratamiento de Datos Personales.

ANÁLISIS COMPARADO

La investigación tiene un enfoque cualitativo, pues se interpreta, a partir del contenido de las legislaciones de Brasil, Cuba, Panamá, Ecuador y Uruguay, los elementos comunes y las diferencias de cinco categorías específicas. El análisis es descriptivo con base en el análisis de las normas.

La metodología comparativa empleada para la investigación seleccionó como sujeto de comparación la legislación de los países que han aprobado o reformado su normativa, posterior a la vigencia del RGPD. Luego, se definieron cinco categorías para la comparación: I. Consentimiento; II. Categorías especiales de datos. III. Flujos transfronterizos de datos. IV. Autoridad de control. VI. Régimen sancionatorio. Finalmente, en cada categoría el análisis específico identifica los elementos comunes de las legislaciones y los factores diferenciadores.

A continuación se muestra la fase descriptiva de las categorías seleccionadas para la comparación y posterior análisis.

Cuadro 1: Países con marco legislativo aprobado / reformado posterior al 2018

CATEGORÍA	NORMA
GDPR	Reglamento General de Protección de Datos 2016/679, emanado del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (GDPR).
CUBA	Ley de Protección de Datos Personales. Aprobada por la Asamblea Nacional del Poder Popular, de 14 de mayo de 2022.
BRASIL	Ley General de Protección de Datos Personales. Ley 13.853 reformatoria de la Ley 13.709.
ECUADOR	Ley Orgánica de Protección de Datos Personales
PANAMA	Ley sobre protección de Datos Personales. Reglamento a la Ley 81.
URUGUAY	Ley de protección de datos personales. Ley reformatoria de la Ley 18.331. Decreto 64/020. Resolución 23-21 del Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales, de 8 de junio de 2021. Resolución 105-2015 del Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales, de 23 de diciembre de 2015.
CATEGORÍA	**I. Consentimiento**
GDPR	Art. 11. Numeral 11).- consentimiento del interesado: toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.
CUBA	Artículo 10. La protección y tratamiento de datos personales se rige por los principios siguientes: l) consentimiento: el titular ha de manifestar su voluntad de forma libre, inequívoca, específica e informada para el tratamiento de los datos personales, precisando el fin con el que se otorga el consentimiento.
BRASIL	Art. 5.- XII. Consentimiento: manifestación libre, informada e inequívoca por la cual el titular está de acuerdo con el tratamiento de sus datos personales para un fin específico.

ECUADOR	Art. 4.- Definiciones.- Consentimiento: Manifestación de la voluntad libre, específica, informada e inequívoca, por el que el titular de los datos personales autoriza al responsable del tratamiento de los datos personales a tratar los mismos. Art. 8.- Consentimiento.- Se podrán tratar y comunicar datos personales cuando se cuente con la manifestación de la voluntad del titular para hacerlo. El consentimiento será válido, cuando la manifestación de la voluntad sea: 1) Libre, es decir, cuando se encuentre exenta de vicios del consentimiento; 2) Específica, en cuanto a la determinación concreta de los medios y fines del tratamiento; 3) Informada, de modo que cumpla con el principio de transparencia y efectivice el derecho a la transparencia, 4) Inequívoca, de manera que no presente dudas sobre el alcance de la autorización otorgada por el titular. El consentimiento podrá revocarse en cualquier momento sin que sea necesaria una justificación, para lo cual el responsable del tratamiento de datos personales establecerá mecanismos que garanticen celeridad, eficiencia, eficacia y gratuidad, así como un procedimiento sencillo, similar al proceder con el cual recabó el consentimiento. El tratamiento realizado antes de revocar el consentimiento es lícito, en virtud de que este no tiene efectos retroactivos. Cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectado para una pluralidad de finalidades será preciso que conste que dicho consentimiento se otorga para todas ellas.
PANAMA	Art. 4. Numeral 4). Consentimiento: manifestación de la voluntad del titular de los datos, mediante la cual se efectúa el tratamiento de estos.
URUGUAY	Art. 4. Literal c). Consentimiento del titular. Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la cual el titular consienta el tratamiento de datos personales que le concierna. Art. 9.- Principio del previo consentimiento informado.- el tratamiento de datos personales es lícito cuando el titular hubiere prestado consentimiento libre, previo, expreso, e informado, el que deberá documentarse. El referido consentimiento prestado deberá figurar en forma expresa y destacada, previa notificación al requerido de datos.

Análisis específico de la categoría:

El consentimiento es un tema estructural y pilar fundamental del sistema de protección de datos y elemento esencial del contenido del derecho (Troncoso 2011), al punto que la ausencia del consentimiento del titular deriva en la ilicitud del tratamiento de los datos personales. El consentimiento refleja el ejercicio de la autodeterminación informativa y constituye la regla general para el tratamiento de los datos personales.

Acorde con los estándares, el consentimiento es caracterizado como: libre, informado e inequívoco, a lo cual adhieren las normas de Brasil, Cuba Ecuador y Uruguay. Por su parte, las normativas de Cuba, Ecuador y Uruguay, siguiendo la línea del GDPR (Trujillo 2017), también incorporan como característica del consentimiento la especificidad, que refiere a la determinación concreta de los medios y fines del tratamiento, por tanto no se puede emplear el consentimiento para el procesamiento de datos a gran escala. La norma panameña es la única que describe el consentimiento en términos generales, como la manifestación de la voluntad del titular de los datos, pero sin precisar las características.

Otro de los elementos comunes es el requerimiento de que el consentimiento sea previo y la admisión de algunas excepciones al requisito de consentimiento, como por ejemplo en caso de realizarse procesamiento de datos para el cumplimiento de un contrato o por disposición de una norma legal.

CATEGORÍA	II. Categorías especiales de datos personales
GDPR	Art. 9. Se prohíbe el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física.
CUBA	Artículo 15.1. Son datos personales sensibles aquellos cuya utilización indebida puede dar lugar a discriminación, implique distinción lesiva a la dignidad humana o conlleve un riesgo grave para su titular. 2. Se incluyen los datos que pueden revelar el sexo, género, identidad, identidad de género, orientación sexual, origen étnico y color de piel, el estado de salud presente o futuro, discapacidad, información genética, u obtenidos a partir de pruebas diagnósticas realizadas en instituciones de salud o vinculadas a las técnicas de reproducción asistida; creencias religiosas e ideológicas; antecedentes policiales y penales. Artículo 16.1. La persona no puede ser obligada a proporcionar datos personales sensibles, ni es lícito su tratamiento sin el consentimiento expreso, inequívoco, libre e informado de su titular, salvo en aquellos casos de excepción previstos en esta Ley. 2. Lo regulado en el apartado anterior se observa también en el caso de personas fallecidas, para lo que se ha de contar con el consentimiento que otorgara en vida, si existe declaración al respecto en el testamento o manifestación de voluntad destinada a ese fin; en su defecto, el de sus herederos o causahabientes.

BRASIL	Art. 5.- II. Datos personales sensibles: datos personales sobre origen racial o étnico, convicciones religiosas, opinión política, afiliación a un sindicato u organización de carácter religioso, filosófico o político, datos relacionados con la salud o la vida sexual, datos genéticos o biométricos, cuando estén vinculados a una persona física. Art. 14. Tratamiento de datos de niños y adolescentes
ECUADOR	Art. 4.- Definiciones.- Datos sensibles: datos relativos a: etnia, identidad de género, identidad cultural, religión, ideología, filiación política, pasado judicial, condición migratoria, orientación sexual, salud, datos biométricos, datos genéticos y aquellos cuyo tratamiento indebido pueda dar origen a discriminación, atenten o puedan atentar contra los derechos y libertades fundamentales. Datos relativos a la salud: datos personales relativos a la salud física o mental de una persona, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud. Art. 25.- Categorías especiales de datos personales.- Se considerarán categorías especiales de datos personales, los siguientes: a) Datos sensibles; b) Datos de niñas, niños y adolescentes; c) Datos de salud; y, d) Datos de personas con discapacidad y de sus sustitutos, relativos a la discapacidad.
PANAMA	Art. 4. Numeral 11. Dato sensible: aquel que se refiera a la esfera íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para este. De manera enunciativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; datos relativos a la salud; a la salud; a la preferencia u orientación sexual; datos genéticos o biométricos; entre otros, sujetos a regulación y dirigidos a identificar de manera unívoca a una persona natural.
URUGUAY	Datos especialmente protegidos: (arts. 18 a 23) Datos sensibles Datos de telecomunicaciones Datos de salud Datos biométricos Datos con fines de publicidad Datos relativos a actividad comercial o crediticia Datos transferidos internacionalmente

Análisis específico de la categoría:
La determinación de categorías de datos personales que requieren mayores o peculiares condiciones o cuidados para su tratamiento es una particularidad nueva de las normas de protección de datos. Se suele enumeran las categorías especiales de datos personales y se determina alguna condición más gravosa para la protección.

En relación con las categorías especiales de datos el elemento común de todas las normas sujeto de la comparación es el relativo a los datos sensibles. Tratándose de éste tipo de datos, el RGPD prohíbe su tratamiento, a diferencia de Cuba y Ecuador que permite el tratamiento pero con el requerimiento especial de contar con el consentimiento expreso del titular. Brasil por su parte prevé un uso más restrictivo de los datos sensibles.

Así también, Ecuador incorpora como categoría especial de tratamiento los datos de niños, niñas y adolescentes, los datos de salud y los datos relativos a las discapacidades. Por su parte, la normativa uruguaya prevé, además, como datos especialmente protegidos a los datos de telecomunicaciones, los datos biométricos, aquellos con fines de publicidad, los relativos a la actividad comercial o crediticia y los datos transferidos internacionalmente.

Cuba, por su parte, adhiere totalmente al lineamiento del GDPR al establecer la correlación de los datos personales sensibles con aquellos cuya utilización indebida puede dar lugar a discriminación, implique distinción lesiva a la dignidad humana o conlleve un riesgo grave para su titular. Destaca, también, que en la enumeración ejemplificativa se incluyan datos genéticos y los relativos a las técnicas de reproducción asistida.

CATEGORÍA	**III. Flujos transfronterizos**
GDPR	Capítulo V. Art. 44 a 49. El principio general de la transferencia internacional de datos personales es la garantía del nivel adecuado de protección en el país, territorio o sector específico al que se transfieren los datos. También es posible realizar la transferencia internacional de datos mediante garantís adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas. Esto incluye las normas corporativas vinculantes, cláusulas tipo, códigos de conducta, mecanismos de certificación.

CUBA

Artículo 63. Se autoriza la transferencia de datos personales dentro del territorio nacional a solicitud de los responsables o encargados de tratamiento de datos, en los casos siguientes:

a) Intercambio de datos de carácter médico, sanitario o investigativo cuando sea requerido para tratamiento del titular, o por interés colectivo;

b) cuando la transferencia de datos tiene como objeto la seguridad colectiva, el bienestar general, el respeto al orden público, y el interés de la defensa;

c) transferencias bancarias en cuanto a las transacciones respectivas;

d) para facilitar el ejercicio del derecho al sufragio en cuanto a la conformación del registro de electores; y

e) por otras razones que de manera significativa así lo ameriten.

Artículo 64. Los responsables o encargados para tratar datos personales, lo son para autorizar su transferencia en el ámbito de sus competencias, cumpliendo los principios establecidos en la presente Ley.

Artículo 65.1. La transferencia internacional de datos a solicitud de la autoridad responsable del país receptor, procede en los casos siguientes:

a) Colaboración judicial internacional;

b) intercambio de datos de carácter médico cuando lo exija el tratamiento del titular, una investigación epidemiológica, en tanto se realice previa adopción de un procedimiento de disociación de la información, con la finalidad de que el titular de los datos sea inidentificable;

c) transferencias bancarias o bursátiles en cuanto a las transacciones respectivas y de acuerdo con la legislación que resulte aplicable;

d) cuando la transferencia se ha acordado en el marco de tratados internacionales en los que la República de Cuba sea Estado Parte; y

e) cuando la transferencia de datos tiene como objeto la cooperación internacional entre organismos para la lucha contra el crimen organizado, el terrorismo, lavado de activos, tráfico de drogas y otros delitos objeto de dicha cooperación;

2. Para autorizar la transferencia internacional de datos se tiene en cuenta la índole o naturaleza de los datos que se solicitan; los fines en los que son utilizados; el consentimiento o información a los titulares en los casos que se requiera; período de duración del tratamiento a que son sometidos o que se tienen previstos; país de origen y destino final de la información; normas de derecho, generales o especiales aplicables; normas profesionales específicas aplicables y medidas de seguridad técnicas y organizativas en vigor en los países de destino.

Artículo 66. El Presidente del Tribunal Supremo Popular, el Fiscal General de la República, el Ministro-Presidente del Banco Central de Cuba y los ministros de Relaciones Exteriores, del Interior, de Justicia y de Salud Pública, están facultados para autorizar la transferencia internacional de datos personales en el ámbito de sus competencias.

BRASIL	Art. 33. Transferencia internacional de datos personales permitida en los casos previstos en la Ley, como a países con nivel adecuado de protección, debiendo dar garantías de cumplimiento de los principios y ser compatible con el régimen de protección de datos de Brasil y que además se cuente con: a) cláusulas contractuales específicas para una transferencia dada; b) cláusulas contractuales estándar; c) estándares corporativos globales; d) sellos, certificados y códigos de conducta emitidos regularmente.
ECUADOR	Capítulo IX. Transferencia o Comunicación Internacional de datos personales. Arts. 55 al 61. Por principio general La transferencia o comunicación internacional de datos personales se podrá realizar a países, organizaciones y personas jurídicas en general que brinden niveles adecuados de protección, y que se ajusten a la obligación de cumplimiento y garantía de estándares reconocidos internacionalmente. El nivel adecuado será determinado por la Autoridad de Protección de Datos Personales. Si no hay nivel adecuado se podrá realizar la referida transferencia internacional siempre que el responsable o encargado del tratamiento de datos personales ofrezca garantías adecuadas para el titular, sustentadas en un instrumento que permita: a. Garantizar el cumplimiento de principios, derechos y obligaciones en el tratamiento de datos personales en un estándar igual o mayor a la normativa ecuatoriana vigente. b. Efectiva tutela del derecho a la protección de datos personales, a través de la disponibilidad permanente de acciones administrativas o judiciales; y, c. El derecho a solicitar la reparación integral, de ser el caso. También se puede realizar transferencia o comunicación internacional de datos personales con base en normas corporativas vinculantes, en cuyo caso se deberá observar el formato y los procedimientos para la transferencia o comunicación de datos realizada en aplicación de las normas corporativas vinculantes.

PANAMA	Art. 33. Se considera lícita la transferencia de datos personales si se cumple al menos con una de las siguientes condiciones: - Consentimiento del titular. - Que el país u organismo receptor proporcione mejor nivel de protección. - Que se encuentre previsto en una Ley o Tratado. - Para prevención de diagnóstico médico. - Que sea efectuada a cualquier sociedad de un mismo grupo económico siempre que no sean usadas para fines distintos. - En virtud de un contrato. - Necesario para la salvaguarda de un interés público. - Para el reconocimiento o defensa de un derecho en un proceso judicial. - Para el mantenimiento o cumplimiento de una relación jurídica. - Requerida para transferencias bancarias o bursátiles. - Para cooperación internacional entre organismos de inteligencia para luchar contra el crimen organizado, terrorismo, narcotráfico, etc. - Que el responsable que transfiere los datos adopte mecanismos de autorregulación vinculante. - En caso de cláusulas contractuales.
URUGUAY	Art. 23.- Datos transferidos internacionalmente. Se prohíbe la transferencia de datos personales de cualquier tipo con países u organismos internacionales que no proporcionen niveles adecuados de protección de acuerdo a los estándares del Derecho Internacional o Regional en la materia. La prohibición no regirá en los casos específicamente detallados en esta disposición. Además, se debe considerar la regulación específica emitida a través de la Resolución de la URCDP N° 23/021

Análisis específico de la categoría:

En la sociedad actual, que debe ser entendida en términos de la Sociedad Red (Amoroso, Nayibe, y otros 2019), los flujos transfronterizos son consustanciales de la protección de datos, puesto que los datos y la información de carácter personal circulan velozmente a través del ciberespacio y las redes que conectan el mundo. Ya en 1990 la Organización de las Naciones Unidas (ONU), en el marco de la Resolución 45/95, consideraba que cuando los países tengan niveles comparables de protección, la circulación transfronteriza debe ser tan libre como dentro de sus propios territorios (Trujillo 2017). En este sentido y como bien ha señalado la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo, los marcos de protección de datos deben ser compatibles

con los flujos de datos internacionales, para que los países en desarrollo puedan beneficiarse de la economía digital mundial.

La transferencia internacional de datos es un tema expresamente previsto en todas las normas sujeto de la comparación, pero con algunas diferencias. La regla común en todas las legislaciones es la posibilidad de realizar transferencia internacional de datos hacia un destino que garantice un nivel adecuado de protección en el país, territorio o sector específico al que se transfieren los datos, a fin de mitigar el riesgo que supone para los derechos de los titulares de los datos la transferencia de datos entre países.

En esa misma línea, otro rasgo común, es la intervención estatal para establecer el nivel adecuado de protección del país de destino, así como el reconocimiento de garantías adecuadas como: las normas corporativas vinculantes, las clausulas tipo los códigos de conducta o los mecanismos de certificación.

Las normas de Brasil, Ecuador y Cuba adhieren a la línea del RGPD, consagrando que el principio general para la transferencia o comunicación internacional de datos personales es el nivel adecuado de protección, o en su defecto si se ofrecen garantías adecuadas. La norma uruguaya prohíbe la transferencia internacional de datos personales si no existen niveles adecuados de protección, excepto en los casos previstos en la misma norma. Por su parte Panamá establece como principio la posibilidad de transferir los datos, con base en las condiciones determinadas en la norma, que no se limita al hecho de que el país u organismo receptor proporcione mejor nivel de protección.

CATEGORÍA	IV. Autoridad de control
GDPR	Capítulo VI. Autoridades de control independientes. Art. 51. Se prevé una autoridad de control creada por cada Estado, creada como autoridad pública independiente.
CUBA	DISPOSICIONES FINALES PRIMERA: Encargar al Ministerio de Justicia el control del cumplimiento de lo dispuesto en la presente Ley. SEGUNDA: El Consejo de Ministros de manera excepcional, autoriza la transferencia internacional de datos personales en los casos no previstos en la presente Ley, a propuesta del Jefe del órgano, organismo de la Administración Central del Estado o entidad nacional que corresponda. TERCERA: Los ministros de las Fuerzas Armadas Revolucionarias y del Interior aplican lo establecido en la presente Ley de acuerdo con las características de sus organismos y adoptan las medidas para modificar, adecuar o dictar las normas que correspondan.

	CUARTA: Los jefes de los órganos, organismos de la Administración Central del Estado y entidades nacionales, establecen las regulaciones internas que correspondan que permitan adoptar las medidas necesarias para dar cumplimiento a lo que por la presente se dispone.
BRASIL	Art. 5. XIX. Autoridad nacional: órgano de la administración pública responsable de fiscalizar, implementar y fiscalizar el cumplimiento de esta Ley en todo el territorio nacional. Art. 1 del Decreto 10.474 de 26 de agosto de 2020. La Autoridad Nacional de Protección de Datos - ANPD, órgano adscrito a la Presidencia de la República, dotado de autonomía técnica y decisoria, con jurisdicción en el territorio nacional y con sede y jurisdicción en el Distrito Federal, tiene como objetivo proteger los derechos fundamentales de libertad y privacidad y el libre desarrollo de la personalidad de la persona natural regidos por lo dispuesto en la Ley N ° 13.709, de 14 de agosto de 2018.
ECUADOR	Art. 4.- Definiciones.- Autoridad de Protección de Datos Personales: Autoridad pública independiente encargada de supervisar la aplicación de la presente ley, reglamento y resoluciones que ella dicte, con el fin de proteger los derechos y libertades fundamentales de las personas naturales, en cuanto al tratamiento de sus datos personales. La Ley no describe expresamente la naturaleza da la Autoridad de Protección de Datos Personales, sin embargo, el artículo 77 hace referencia al Superintendente de Protección de Datos como titular de la misma. Se deduce, por tanto, la existencia de una Superintendencia, entidad que se crea al amparo de lo establecido en la Constitución de la República, que en su artículo 213 señala que las superintendencias son organismos técnicos de vigilancia, auditoría, intervención y control de las actividades económicas, sociales y ambientales, y de los servicios que prestan las entidades públicas y privadas, con el propósito de que estas actividades y servicios se sujeten al ordenamiento jurídico y atiendan al interés general. Son parte de la Función de Transparencia y Control Social, pero de conformidad con el Art. 204 de la Constitución de la República, son entidades con personalidad jurídica y autonomía administrativa, financiera, presupuestaria y organizativa.

	Además, el Art. 205 de la Constitución determina que los representantes de las entidades que forman parte de la Función de Transparencia y Control Social, entre las que se cuentan las superintendencias, tienen fuero de Corte Nacional y están sujetos al enjuiciamiento político de la Asamblea Nacional. Su selección se realiza mediante concurso público de oposición y méritos en los casos que proceda, con postulación, veeduría e impugnación ciudadana. Esto da cuenta de la independencia de la autoridad que represente a la Superintendencia de Protección de Datos.
PANAMA	Art. 34. Consejo de Protección de Datos Personales. Ente consultivo en materia de protección de datos. Art. 36. La Autoridad Nacional de Transparencia y Acceso a la Información es el ente que podrá aplicar las sanciones.
URUGUAY	Artículos del 31 a 34. Unidad Reguladora y de Control de Datos Personales.

Análisis específico de la categoría:

La existencia de una autoridad de control en materia de protección de datos es uno de los pilares fundamentales en el sistema de protección de los datos y lo que caracteriza la particularidad única del derecho a la protección de datos, que a diferencia de otros derechos, cuenta con una autoridad exclusiva para velar por su respeto y no vulneración. Tal premisa es condición necesaria más no suficiente, pues las características de autonomía, independencia e imparcialidad en la actuación de la autoridad de control determinarán el cumplimiento del estándar internacional (Guerrero 2019).

La autonomía no es la característica que define a los organismos de control de protección de datos previstos en las legislaciones sujeto de la comparación, como se puede evidenciar respecto de la autoridad de control de Brasil, Panamá y Uruguay. La autoridad brasileña está adscrita a la Presidencia de la República; la autoridad uruguaya tiene autonomía técnica pero es un órgano desconcentrado de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y de la Sociedad de la Información y del Conocimiento (AGESIC); y, en el caso de Panamá el Consejo de Protección de Datos Personales funge únicamente como ente consultivo, siendo la Autoridad Nacional de Transparencia y Acceso a la Información el ente que puede aplicar las sanciones. Finalmente, la norma cubana encarga el cumplimiento de la misma al Ministerio de Justicia y reparte competencias a otros funcionarios de Estado, por tanto destaca el hecho de que la norma no haya creado ninguna entidad especializada.

El caso de Ecuador es diferente, puesto que la Superintendencia de Protección de Datos, conforme a las disposiciones Constitucionales, será una entidad con personalidad jurídica y autonomía administrativa, financiera, presupuestaria y organizativa. Esta autonomía también corresponde a la figura de su representante, esto es el Superintendente, que

deriva del proceso de selección, así como de la imposibilidad de su destitución, salvo el caso de que se realice un juicio político en la Asamblea Nacional. Por lo tanto, la autoridad ecuatoriana es la única que cumple con el estándar de independencia y autonomía.

CATEGORÍA	V. Régimen sancionatorio
GDPR	Art. 83. Condiciones generales para la imposición de multas administrativas. Art. 84. Los Estados deben definir las demás sanciones aplicables por las infracciones cometidas. Las sanciones serán efectivas, proporcionadas y disuasorias.
CUBA	Sección Cuarta Del incumplimiento de las disposiciones relativas a la protección de datos personales. Artículo 56.1. Las personas naturales o jurídicas, sujetas al régimen legal que esta Ley establece, que incumplan las disposiciones relativas a la protección de datos personales se les imponen, por la autoridad competente, las sanciones y medidas siguientes: a) Apercibimiento; b) multa de hasta 20 000 pesos; c) suspensión de la base de datos respectiva por el plazo de hasta cinco días; y d) clausura de la base de datos. 2. Estas sanciones y medidas se gradúan teniendo en cuenta el impacto social, la gravedad, reiteración o reincidencia de la infracción cometida. 3. Las sanciones y medidas se aplican sin perjuicio de la responsabilidad civil o penal en la que se pueda incurrir. 4. La autoridad competente para imponer la multa y demás medidas que correspondan por los incumplimientos de las disposiciones relativas a la protección de datos personales, son los funcionarios autorizados expresamente por los órganos, organismos de la Administración Central del Estado y entidades nacionales, en el ámbito de su competencia. Artículo 57.1. Contra la sanción o medida impuesta por la autoridad competente el afectado puede interponer por escrito recurso de apelación en el plazo de 10 días hábiles siguientes a la fecha de notificación. 23.2. Está facultado para conocer y resolver el recurso de apelación, el jefe inmediato superior de la autoridad que impuso la sanción o medida. 3. Con el recurso de apelación el inconforme propone las pruebas de que intente valerse a los fines de su impugnación.

	Artículo 58. El jefe inmediato superior que conoce del recurso puede convocar al recurrente para ser escuchado sobre su impugnación. Artículo 59. El recurso de apelación no interrumpe la ejecución de la sanción o medida impuesta. Artículo 60.1. El recurso se resuelve en un plazo de hasta diez días hábiles posteriores a su presentación. 2. Dicho plazo puede ser prorrogado por diez días hábiles más si la práctica de pruebas presentadas lo hace necesario. 3. La resolución que resuelve el recurso de apelación se notifica al recurrente dentro del plazo de tres días hábiles siguientes a la fecha de dictada. Artículo 61. En el caso en que se declare con lugar el recurso, la decisión se comunica a quienes hayan intervenido en la ejecución de la sanción o medida. Artículo 62. Contra la decisión de la autoridad administrativa facultada procede demanda administrativa en sede judicial.
BRASIL	Art. 52. Sanciones administrativas: Advertencia, indicando el plazo para tomar las medidas correctivas; multa simple de hasta el 2% (dos por ciento) de los ingresos de una persona jurídica de derecho privado, grupo o conglomerado en Brasil en su último año fiscal, sin impuestos, limitada en total a R $ 50.000.000,00 (cincuenta millones de reales) por infracción; multa diaria, observando el límite total a que se refiere el ítem II; dar a conocer la infracción después de que su ocurrencia sea debidamente investigada y confirmada; bloqueo de los datos personales a los que se refiere la infracción hasta su regularización; supresión de los datos personales a los que se refiere la infracción; suspensión parcial del funcionamiento de la base de datos a la que se refiere la infracción por un período máximo de 6 (seis) meses, prorrogable por igual período, hasta la regularización de la actividad de tratamiento por parte del responsable del tratamiento; Prohibición total o parcial del ejercicio de actividades relacionadas con el tratamiento de dato.
ECUADOR	Capítulo XI. Medidas correctivas, infracciones y régimen sancionatorio. Artículos 65 al 74. Sección 1ª. Se establecen infracciones leves y graves en las que incurren tanto los responsables como los encargados del tratamiento de datos personales. Se establecen las sanciones aplicables para las infracciones leves y para las graves.

PANAMA	Art. 36. Sanciones pecuniarias acorde a la gravedad de las faltas que se establecerán desde mil balboas así como diez mil balboas. Art. 43. Sanciones: Faltas leves: citación ante la Autoridad Nacional de Transparencia y Acceso a la Información. Faltas graves: multas según su proporcionalidad. Faltas muy graves: clausura de los registros de la base de datos, sin perjuicio de la multa correspondiente. Suspensión e inhabilitación de la actividad de almacenamiento y/o tratamiento de datos personales de forma temporal o permanente.
URUGUAY	Art. 35. URCDP. Observación Apercibimiento Multa Suspensión de la Base de Datos Clausura de la Base de Datos Resolución de la URCDP N° 105/015 (reglamenta la aplicación de las sanciones)

Análisis específico de la categoría:
El sistema de protección de datos prevé como un pilar para el cumplimiento un régimen sancionatorio, que incluye diferentes tipos de medidas que se aplican según el tipo y gravedad de la falta.

Tratándose del régimen sancionatorio las similitudes se establecen por la existencia de sanciones administrativas y pecuniarias, pero con cuantías diferentes que se ubican en extremos y medidas de diferente tipo. Pero, destaca que las normas en comparación en términos de sanciones pecuniarias tienen límites menos rigurosos que el GDPR.

CONCLUSIONES

Desde la década del 70 del siglo XX, progresivamente, se supera el concepto restringido de derecho a la intimidad. Este, aplicado a los avances tecnológicos actuales, da paso a la denominación de derecho a la autodeterminación informativa o libertad informática y años más tarde emerge como un derecho autónomo e independiente denominado derecho a la protección de datos personales.

La diversidad de criterios expuestos en estos últimos años, con independencia de los elementos que cada uno de ellos tuvo en cuenta para ofrecer una conceptualización del derecho a la protección de datos personales ha permitido determinar que debe ser entendido como aquel a través del cual se aseguran todos aquellos datos de carácter personal, que identifiquen o sean susceptible de identificación y a tal efecto le ocasionen alguna afectación al titular de los mismos. En consecuencia, el titular podrá solicitar el acceso, la rectifica-

ción, cancelación u oponerse al tratamiento y uso de sus datos. De ahí que la intensificación de los riesgos que la compilación y sistematización de los datos de carácter personal ha provocado con el auge creciente de las tecnologías de la información y las comunicaciones permitiera clarificar las diferencias entre lo reconocido como derecho a la intimidad, el derecho a la autodeterminación informativa o libertad informática y el derecho a la protección de datos personales.

Latinoamérica ha seguido la línea del sistema europeo de protección de datos, en cuanto al reconocimiento del derecho a la protección de datos y la necesidad de garantizarlo, desde la perspectiva de los derechos humanos. Sin embargo, en relación al marco jurídico-legal del derecho a la protección de datos ha tenido una evolución asimétrica, pudiendo identificarse países con una normativa adecuada, en términos del estándar europeo, así como países con un nivel de protección mínimo.

El panorama normativo de protección de datos en Latinoamérica ha tenido cambios significativos a partir del 2018, en razón de la aprobación y vigencia del Reglamento de la Unión Europea 2016/679, emanado del Parlamento Europeo y del Consejo el 27 de abril de 2016. Esto debido a los efectos que dicha normativa conlleva, incluso, fuera del espacio europeo, siendo este un aspecto relevante para los países que mantienen fuertes lazos comerciales con la Unión Europea

Muchos de los países de Latinoamérica que no contaban con legislación de protección de datos, están trabajando en sendos proyecto de leyes de protección de datos, tomando como referente el RGPD. Esto implica una clara postura de Latinoamérica en el sentido de cumplir los estándares internacionales para la protección de datos personales. Sin embargo, no ha sido posible avanzar en relación con la estandarización de la normativa de protección de datos a nivel Latinoamericano. Por el contrario, el panorama de Latinoamérica se torna complejo, debido a las particularidades que los Estados que han aprobado normas específicas de protección de datos han introducido en su legislación interna, tal como se evidencia en el análisis comparativo de las cinco categorías referidas en este trabajo.

TRABAJOS CITADOS:

Amoroso, Yarina. «Contribución al debate sobre la protecccón de datos personales en Cuba.» *GIGA*, nº 2 (2019).

___. ¿Qué desafíos trae la nueva Ley de Protección de Datos?. *CUBAHORA.* 2022.

Amoroso, Yarina, Chacón Nayibe, García Myrna, y Guerrero, Patricia, Reyes Jacqueline. *Gobierno de la Información: realidades contemporáneas.* Quito: UDLA, 2019.

Baños, José María. «Ley de Protección de Datos Brasil: un panorama general de la nueva legislación.» *letslaw.* 6 de mayo de 2019. https://letslaw.es/ley-de-proteccion-de-datos-brasil/ (último acceso: 15 de agosto de 2021).

Bustamante, Javier. «La cuarta generación de derechos humanos en las redes digitales.» *TELOS. Caudernos de Comunicación e Innovación*, 2010.

Castell, Manuel. *Informations, reseaux, identitees Les clés du XXIe siécle.* París: Fayard, 2002.

Castells, Mercedes. «Uruguay dicta nuevas normas sobre protección de datos.» *IAPP - The International Association of Privacy Professionals.* 7 de abril de 2020. https://iapp.org/news/a/uruguay-dicta-nuevas-normas-sobre-proteccion-de-datos/ (último acceso: 21 de agosto de 2021).

Cutié, Daniela. *El sistema de garantías de los derechos humanos en Cuba (tesis doctoral).* Santiago de Cuba: Uni-

versidad de Oriente, 1999.

De la Guardia, Mariela. «Protección de Datos en Panamá.» *Icaza González-Ruiz y Alemán.* 8 de junio de 2021. https://www.icazalaw.com/wp-content/uploads/2021/07/MEMO-PROTECCION-DE-DATOS-EN-PANAMA-1-de-julio-de-2021.pdf (último acceso: 15 de septiembre de 2021).

Delpiazzo, Carlos. «Facilitación del Comercio Electrónico por el Derecho uruguayo.» *Comercio Electrónico* (Faira), 2003.

García González, Aristeo. «La protección de datos personales: derecho fundamental del siglo XXI. Un estudio comparado.» *Boletín mexicano de Derecho comparado.* XL, nº 120 (sept-dic 2007).

García, Aristeo. «La protección de datos personales: derecho fundamental del siglo XXI. Un estudio comparado.» *Boletín mexicano de Derecho comparado* 40, nº 120 (2007).

Guerrero, Jacqueline. «La autoridad de control de protección de datos. Condiciones para la efectividad del sistema de protección.» En *El Derecho de las TIC en Iberoamérica*, de Dir Marcelo Bauzá. Montevideo: La Ley, 2019.

OEA. «Estudio comparativo: protección de datos en las Américas.» 2012.

Ojeda Bella, Zahira y Yarina Amoroso. «La protección de los datos personales en Cuba desde la legislación vigente.» *Revista Justicia Juris* 12, nº 2 (2016): 88-89.

Ojeda Bello, Zahira. «Tesis doctoral.» *El derecho a la protección de datos personales.* 2020.

Pérez Luño, Antonio. *Derechos Humanos, Estado de Derecho y Constitución.* Madrid, 1991.

—. *Los derechos humanos en la sociedad tecnológica.* Lima: Comisión Andina de Juristas, 1994.

Puccinelli, Oscar. *El Habeas Data en Indoiberoamérica.* Colombia: Temis, 1999.

Troncoso, Antonio. *La protección de datos personales. En búsqueda del equilibrio.* Madrid: Tirant to Blanch, 2011.

Trujillo, Carlos. «Aproximación a la regulación del consentimiento en el Reglamento General de Protección de Datos.» *Anales de la Facultad de Derecho* (Universidad de la Laguna), 2017: 67 - 75.

Villabella, Carlos Manuel. *Estudios de Derecho Constitucional.* La Habana: UNIJURIS, 2020.