CELE

Iniciativas legislativas sobre privacidad y protección de datos en Argentina, Brasil, Chile, Colombia, Ecuador, México, Guatemala, Paraguay y Perú, período 2019-2021

Septiembre 2022

Facultad de Derecho
Centro de Estudios en Libertad
de Expresión y Acceso a la Información

UP
Universidad
de Palermo

Iniciativas legislativas sobre privacidad y protección de datos en Argentina, Brasil, Chile, Colombia, Ecuador, México, Guatemala, Paraguay y Perú, período 2019-2021

Olga Lucía Camacho Gutiérrez* *y Lina Paola Velásquez Veloza*****
CELE

I. Introducción

Casi siempre se advierte que la regulación suele ir en rezago frente a los retos que proponen las nuevas tecnologías digitales y la transformación continua de internet. Sin valorar si el derecho debería o no formular un marco regulatorio para cada nueva tecnología que surge a diario, aquella es una consideración que, en todo caso, debiera poder incentivar la formulación de legislaciones comprehensivas capaces de responder a través de la adopción de los estándares en derechos humanos, del ejercicio de derechos en ambientes o de las herramientas que conservan una arquitectura y una lógica propias, pero que entrañan conflictos que no nos resultan del todo desconocidos.

En materia de privacidad y protección de datos, la formulación de estándares de ese tipo, que resultan aplicables a su ejercicio en internet y de cara al uso de tecnologías digitales, no es reciente en nuestra región. Llevan siendo advertidos con insistencia desde el inicio de la década anterior, cuando los eventos de abusos a los sistemas de vigilancia de las comunicaciones en la región, así como el creciente despliegue de internet y el protagonismo de las empresas de telecomunicaciones, pusieron de presente los efectos nocivos de la desactualización o inexistencia de normativa capaz de facilitar los procesos de rendición de cuentas y la vigencia de garantías para la defensa y la protección de las personas.

Seguir insistiendo en lo obvio una década después, es decir, en la adopción de los mismos estándares, debe poder activar procesos de reflexión para evaluar de

* Consultora del Observatorio Legislativo del CELE Palermo.

** Asistente de investigación del Observatorio Legislativo del CELE Palermo.

cerca cuál es el verdadero estado de la regulación de cara a los nuevos (viejos) retos que proponen nuevos medios y escenarios digitales, y que debería poder llevar a responder las preguntas sobre qué ha faltado para lograr su adopción, qué se precisa y cuáles deberían ser los enfoques para producir el cambio legislativo que se requiere en cada país. Para contribuir a dicho proceso, el Observatorio Legislativo del Centro de Estudios para la Libertad de Expresión y Acceso a la Información (CELE) de la Universidad de Palermo –en adelante, el "Observatorio Legislativo"– se ha propuesto ampliar el alcance de su trabajo de monitoreo legislativo en materia de libertad de expresión, para cubrir los temas de privacidad y protección de datos en algunos países de la región. El objetivo de la nueva matriz de información del Observatorio Legislativo, así como el de este informe, es servir como insumo de carácter comparativo para reconocer experiencias y rezagos que faciliten la articulación de esfuerzos de incidencia para el avance de una mejor regulación en cada país.

Para ello, este informe recoge en la primera parte algunas de las preocupaciones y progresos de la última década en ambos temas, que han sido señalados en los análisis de distintas organizaciones de la sociedad civil dedicadas a la investigación y a la incidencia en derechos digitales y libertad de expresión en la región. En la segunda parte, se recogen de manera sintética los estándares regionales en derechos humanos aplicables a la protección de datos y a la privacidad, con el fin de proveer un marco de análisis que sirva a la revisión de la actividad legislativa de los nueve países de interés para este informe. En la tercera parte, se revisan los avances legislativos de cada uno de los nueve países. Se cierra con algunas conclusiones sobre la continuidad de este informe y los retos que siguen para ejercicios de observación legislativa en ambos temas.

II. Metodología

La recolección de la información se orientó en dos criterios de delimitación, uno temporal y otro geográfico. El temporal, que cubre la búsqueda de proyectos de ley y leyes desde enero de 2019 hasta septiembre de 2021. Y el geográfico, que cubre solo a nueve países de la región latinoamericana: Argentina, Brasil, Chile, Colombia, Ecuador, Guatemala, México, Paraguay y Perú, que son, a su vez, los países en los que el Observatorio Legislativo ha enfocado su actividad de monitoreo en materia de libertad de expresión.

La búsqueda de información se apoyó, en primer lugar, en la consulta y en el barrido de los sitios web oficiales de los Congresos de cada país, así como en sus gacetas legislativas. Frente a las dificultades asociadas a la transparencia de la actividad legislativa[1] en varios de estos, se acudió, en un segundo lugar, a los informes o a las noticias de la actividad legislativa relacionados a la protección de datos y a la privacidad producidos por algunas organizaciones de la sociedad civil, entre las que se incluyó a la Asociación por los Derechos Civiles en Argentina; a la Fundación Karisma en Colombia; a Derechos Digitales en Chile; a InternetLab y Data Privacy en Brasil; a Usuarios Digitales en Ecuador; a R3D en México; a Tedic en Paraguay; y a Hiperderecho en Perú. La información relevada luego fue sistematizada en la matriz de leyes y proyectos de ley en la que fue caracterizada según un conjunto de criterios generales o identificatorios de las iniciativas, y según un conjunto de criterios sobre su contenido que se orienta conforme a los estándares del sistema interamericano y a los llamados de atención de la última década sobre el balance de deudas o retos pendientes en cada uno de los dos temas (que se abordan en la siguiente sección).

Ahora bien, es importante advertir diversos aspectos asociados al alcance y al enfoque de la metodología propuesta que impactan asimismo en el sentido del informe. El primero de ellos se asocia al carácter no exhaustivo de la caracterización de las leyes y de los proyectos de ley sobre protección de datos y privacidad. El objetivo de los criterios de caracterización de este informe constituye más bien una propuesta inicial para uniformizar y proveer elementos de base para el acercamiento a los proyectos de ley y leyes mapeados, que regulan o proyectan regular la protección de datos y privacidad en cada uno de los nueve países revisados. Este proceso se enfrenta, en todo caso, a las condiciones de técnica legislativa de cada país en donde el contenido de una iniciativa puede tratar ambos temas a la vez, por ejemplo. La segunda advertencia comprende la diferenciación y la agrupación de las leyes y de los proyectos de ley en materia de privacidad, por un lado, y de protección de datos, por el otro.

Bajo el paraguas de la protección de datos, se incluyeron las iniciativas y leyes que, de manera integral o con algunas previsiones, comprenden el procesamiento de datos personales, sin importar que legislativamente hayan sido o no tituladas como leyes o proyectos de ley de protección de datos. En este grupo, se integraron

[1] Según el más reciente índice de transparencia legislativa, ningún país, con excepción de Chile, obtuvo más de 50 puntos en materia de transparencia y apertura. Esta situación se ve reflejada en aspectos prácticos como el acceso y la accesibilidad de la información, así como en su publicación y actualización continua, entre otros. Ver, Red Latinoamericana por la Transparencia Legislativa, "Índice latinoamericano de transparencia legislativa", Eurosocial, 5a ed., 2020, disponible en: https://www.transparencialegislativa.org/indice-2020, último acceso: 10 de abril de 2022.

a todas las que aluden a las facultades de la persona para controlar su información personal y las reglas que orientan el procesamiento de sus datos personales.

Bajo el paraguas de la privacidad, se incluyeron las regulaciones que, de manera integral o con algunas previsiones, refieren a la regulación que protege o limita los cuatro bienes jurídicos[2] que amparan dicho derecho, que incorporan, pero no se limitan a la legislación sobre la vigilancia masiva o individualizada de las comunicaciones. Se identificaron leyes y proyectos de ley sin importar si el título de la regulación refería o no a la privacidad como derecho regulado.

De esta manera, este informe reconoce que la protección de datos y la privacidad, sea que se las regule como derechos autónomos o uno cobijado como facultad del otro, apuntan conjuntamente a la protección de valores similares –como la autonomía de la persona y el libre desarrollo de su personalidad– y constituyen un prerrequisito para el ejercicio de otros derechos fundamentales –como la libertad de expresión y la libertad de libre asociación y protesta, entre otros–. Por ello, y pese a la diferenciación propuesta, puede que en ocasiones la misma no sea en todos los casos tajante.

III. Protección de datos y privacidad: balance de preocupaciones sobre el estado de la regulación en cada materia

Diversos informes y análisis comparativos se han emprendido para revisar el estado de la regulación en protección de datos y privacidad en los nueve países en que se centra este informe, los cuales resultan pertinentes para poder comprender las discusiones actuales. Se trata de textos que permiten proveer un contexto sobre algunos de los avances y retos que han impactado en la agenda legislativa sobre estos temas, que recogemos a continuación (sin ánimo exhaustivo), en tanto que influyeron en la caracterización de los proyectos y leyes sobre protección de datos y privacidad en la nueva matriz de información del CELE.

Para esta revisión de contexto, sugerimos, en lo que sigue, una revisión temporal comprendida en la década de 2010 a 2020, pues se trata de un espectro de tiempo generoso que permite ver de cerca la permanencia de algunos retos, así como poner de presente la lentitud y la progresividad con que se han reportado algunos avances. Veamos.

[2] El primero, el de contar con una esfera personal para la toma de decisiones libres sobre la propia vida. El segundo, tener un espacio de tranquilidad personal. El tercero, mantener reservados aspectos de la vida privada. Y el último, controlar la difusión de la información personal hacia terceros. Sobre este aspecto proveemos una visión ampliada en la sección de estándares en DDHH.

1. Tendencias en la década 2010-2020

Algunos análisis de regulación en la región[3] apuntan a la existencia de un modelo latinoamericano sobre la base del reconocimiento constitucional del derecho a la privacidad y *habeas data*, influido en buena medida por el sistema europeo. A nivel constitucional en buena parte de los países de América Latina, y con algunos matices,[4] se había reconocido hasta la primera década del siglo XXI el derecho a la protección de datos y privacidad. Se trataba de previsiones que podían leerse en las Constituciones políticas de El Salvador, artículo 2 (1983); Brasil, artículo 5, numeral 68 (1988); Colombia, artículo 15 (1991); Paraguay, artículo 33 (1992); Perú, artículo 2, numeral 6 (1993); Guatemala, artículo 24 (1993); Argentina, artículo 43 (1994); Venezuela, artículo 28 (1999); Panamá, artículos 42 y 44 (2004); Ecuador, artículo 66, numeral 19 (2008); por mencionar tan solo algunos países.

---

[3] Villegas Carrasquilla, Lorenzo, "Protección de datos personales en América Latina: retención y tratamiento de datos personales en el mundo de internet", en: Bertoni, Eduardo (comp.), *Hacia una internet libre de censura: propuestas para América Latina*, Buenos Aires, CELE, 2012, pp. 125-164, disponible en: https://www.palermo.edu/cele/pdf/internet_libre_de_censura_libro.pdf, último acceso: 10 de abril de 2022; Cerda Silva, Alberto J., "Protección de datos personales y prestación de servicios en línea en América Latina", en: Bertoni, Eduardo (comp.), *Hacia una internet libre de censura: propuestas para América Latina*, Buenos Aires, CELE, 2012, pp. 165-180, disponible en: https://www.palermo.edu/cele/pdf/internet_libre_de_censura_libro.pdf, último acceso: 10 de abril de 2022; Remolina Angarita, Nelson, "Aproximación constitucional de la protección de datos personales en Latinoamérica", en: *Revista Internacional de Protección de Datos Personales (RIPDP)*, N° 1, Bogotá, 2012, pp. 4-13, disponible en: https:/habeasdatacolombia.uniandes.edu.co/wp-content/uploads/7_-Nelson-Remolina.pdf, último acceso: 10 de abril de 2022; Cerda Silva, Alberto, "El 'nivel adecuado de protección' para la transferencia de datos personales desde la Unión Europea", en: *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso*, N° 36, 1er semestre, Valparaíso, 2011, pp. 327-356, disponible en: https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-68512011000100009, último acceso: 10 de abril de 2022.

[4] Con verbalizaciones que distan en lo formal, se habían adoptado a nivel constitucional tres tipos de reconocimiento constitucional hasta entonces. El primero, de reconocimiento explícito del derecho de protección de datos; el segundo, de reconocimiento explícito del recurso de *habeas data* para la protección de la información íntima o personal; y el tercero, de reconocimiento constitucional explícito al derecho a la intimidad y a la privacidad. Ver, Zamudio Salinas, María Lourdes, "El marco normativo y la Ley de Protección de Datos del Perú", en: *Revista Internacional de Protección de Datos Personales (RIPDP)*, N° 1, Bogotá, 2012, pp. 4-21, disponible en: https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/ok3_Ma.-de-Lourdes-Zamudio_FINAL.pdf, último acceso: 10 de abril de 2022. También creemos que existe un cuarto modelo de reconocimiento implícito, mucho más débil o incompleto en comparación con el resto, de protección exclusiva a la inviolabilidad de las telecomunicaciones y la correspondencia personal.

En opinión de Katitza Rodríguez: "La Constitución de cada país latinoamericano reconoce el derecho a la privacidad de cierta forma: comúnmente como un derecho general a la vida privada o intimidad. A veces es protegido como múltiple, derechos específicos: el derecho a la inviolabilidad de las comunicaciones; como el derecho a la protección de datos o el derecho de hábeas data, que varía de un país a otro, pero en general, el hábeas data protege el derecho de toda persona a conocer la información que se guarda sobre su persona". Ver, Rodríguez, Katitza, "Análisis comparado de las leyes y prácticas de vigilancia en América Latina", Necesarios & Proporcionados, Electronic Frontier Foundation (EFF), 2016, disponible en: https://necessaryandproportionate.org/es/comparative-analysis-surveillance-laws-and-practices-latin-america/#resumen-ejecutivo, último acceso: 10 de abril de 2022.

1.1. Protección de datos

Pese a dicho reconocimiento, sólo algunos países habían adoptado, hasta 2010, legislaciones generales de protección de datos: Chile (ley N° 19.628, 1999), Argentina (ley N° 25.326, 2000), Uruguay (ley N° 18.331, 2008) y México (Ley Federal de Protección de Datos Personales, 2010). En Paraguay (ley N° 1.682, 2001) y Colombia (ley N° 1.266, 2008), se habían adoptado regímenes especiales para el sector financiero.

A inicio de la década, se identificaron retos en materia de diseño legal esencialmente en tres temas: los de su aplicabilidad y alcance; los de actualización de su contenido; y los de fortalecimiento de los mecanismos de supervisión y aplicación. Sobre su aplicabilidad y alcance, por ejemplo, se apuntó entonces a la necesidad de superar el criterio de jurisdicción atado a los aspectos territoriales para poder centrarse en la persona en aras de ofrecerle protección ante el indebido manejo de sus datos, sin importar en dónde estuviera domiciliada la empresa responsable de dicho tratamiento. Los requerimientos relacionados con la actualización de su contenido incluyeron la mención del reconocimiento de estándares que hicieran posible la transferencia y la recolección internacional de datos bajo niveles adecuados de protección (casos de Chile y Colombia), la adopción más amplia del consentimiento como la base legal del tratamiento y su adecuación de cara a las dinámicas de internet (Colombia y Paraguay), hasta la evaluación de la viabilidad de regímenes de responsabilidad en el tratamiento de datos en internet compatibles con los estándares de libertad de expresión. Las menciones asociadas al fortalecimiento de los mecanismos de supervisión y aplicación de la ley llamaban la atención sobre la necesidad de crear autoridades de protección de datos, así como vías para garantizar su exigibilidad.

A mediados de la década, diversos informes comparativos[5] recogían buena parte de estos retos, y enfatizaban en la importancia que tenía para la región llevar a cabo procesos de armonización legislativa, de fortalecimiento de los mecanismos de exigibilidad y de cumplimiento del derecho a la protección de datos, y la

[5] Ucciferri, Leandro, "El sistema de protección de datos personales en América Latina: oportunidades y desafíos para los derechos humanos – vol. I", Asociación por los Derechos Civiles (ADC), 2016, disponible en: https://adc.org.ar/informes/sistema-proteccion-datos-personales-latam, último acceso: 10 de abril de 2022; Ucciferri, Leandro, "Políticas de protección de datos personales en las empresas de telecomunicaciones: estudios de casos de Argentina, Brasil, Chile y México – vol. II", ADC, 2016, disponible en: https://adc.org.ar/informes/politicas-proteccion-datos-personales-empresas-telecomunicaciones, último acceso: 10 de abril de 2022; y Milanés, Valeria, "Desafíos en el debate de la protección de datos en Latinoamérica", en: *Revista Transparencia y Sociedad*, N° 5, Santiago de Chile, 2017, pp. 13-31, disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=6245758, último acceso: 10 de abril de 2022.

separación en el tratamiento regulatorio de los asuntos de protección de datos, por un lado, y privacidad, por el otro. En 2018, la entrada en vigencia del Reglamento General de Protección de Datos en Europa marcó un hito en la adopción de estándares elevados y de diseño regulatorio en dicha materia, lo que fijó en adelante un modelo a imitar en la región. Tal fue el caso en iniciativas que luego se transformaron en ley en Brasil, Paraguay y más recientemente en Ecuador, las cuales adoptan en mayor o menor medida algunos estándares y buenas prácticas recogidas por dicho reglamento. Este hito estuvo antecedido por otros desarrollos de carácter regional, como la creación de los "Estándares de protección de datos personales" a cargo de la Red Iberoamericana de Protección de Datos,[6] y la primera versión de los "Principios interamericanos sobre privacidad y protección de datos",[7] entre otros.

1.2. Privacidad

Sobre los retos de confección regulatoria advertidos a inicio de la década, se identificó la necesidad de proveer estándares para la protección de la persona en las actividades de retención y compartición de los datos de los usuarios y de las usuarias de los servicios de las empresas de internet y telecomunicaciones, que hasta entonces era incipiente; de estándares en derechos humanos para la regulación de las actividades de interceptación y vigilancia de las comunicaciones. Se trata de actividades frente a las que la protección de datos, como herramienta orientada al control de la información personal, es esquiva para dar respuestas suficientes y adecuadas.[8]

Este conjunto de preocupaciones sería objeto del trabajo intenso de la sociedad civil que, a mitad de la década, emprendió dos tareas. Por una parte, la emisión, por países, de informes dirigidos a evaluar los compromisos de las empresas de telecomunicaciones y algunas plataformas de internet en la protección de la privacidad de sus suscriptores y suscriptoras. Por otra parte, el análisis y la difusión de informes comparativos en diversos países sobre los marcos regulatorios de las actividades de interceptación y vigilancia de las comunicaciones.

---

[6] Red Iberoamericana de Protección de Datos, "Estándares de protección de datos personales para los Estados iberoamericanos", 2017, disponible en: https://www.redipd.org/es/documentos/estandares-iberoamericanos, último acceso: 10 de abril de 2022.

[7] Organización de Estados Americanos (OEA), Comité Jurídico Internacional (CJI), "Guía legislativa sobre la privacidad y la protección de datos personales en las Américas", 2015, disponible en: https://www.oas.org/es/sla/ddi/proteccion_datos_personales_Guia_Legislativa_CJI_2015.asp, último acceso: 10 de abril de 2022.

[8] Cerda Silva, *supra* nota 3.

Producto de la primera tarea,[9] de manera unánime, se ha realizado desde entonces un llamado de atención sobre la necesidad de mejores prácticas de transparencia sobre los tipos de datos accedidos por las autoridades (que exigen claridad e información sobre los tiempos y tipos de datos que son retenidos por las empresas de telecomunicaciones), y sobre el procedimiento en torno a dichas solicitudes (que exigen claridad e información sobre el número de solicitudes de entrega de dichos datos elevados por las autoridades, el número de solicitudes de interceptación de las telecomunicaciones que reciben y tramitan, una relación de las solicitudes de entrega de datos que proceden y las que no, la descripción del procedimiento de su entrega, la notificación a la persona afectada, etc.).

Producto de la segunda tarea, se efectuó un diagnóstico regional[10] que, más allá de reiterar el papel que juegan en materia de transparencia los Estados y las empresas de telecomunicaciones y que debía poder fortalecerse, expuso los riesgos asociados al rompecabezas legislativo de estos temas cuya dispersión, vaguedad y ambigüedad en su contenido tornan a la regulación existente en un escenario propicio para el abuso. En dicho diagnóstico de alcance regional, por ejemplo, se identificó una taxonomía compleja y confusa sobre los tipos de información protegida que podía estar sujeta a las actividades de inteligencia y vigilancia. Se identificó como un factor común la desactualización legislativa, la cual no permitía responder a los retos que plantean internet y otras tecnologías digitales que facilitan las actividades de vigilancia masiva de las comunicaciones. Asimismo, se hizo mención a la ausencia de mecanismos de supervisión pública, de notificación a la persona afectada y de recursos efectivos para facilitar el reclamo ante abusos.

En su análisis, y en la misma línea, Carlos Cortés Castillo se refería entonces a la brecha regulatoria entre las avanzadas capacidades de la vigilancia de las comunicaciones de los Estados y la debilidad de los controles que reflejaban marcos jurídicos como el colombiano y el chileno.[11] La condición dispersa de la regula-

[9] Se trata de la versión modificada del informe "Who Has your Back?" de la Electronic Frontier Foundation (EFF), que ha recibido en la región diversos nombres, pero que apunta, en general, a evaluar los compromisos en derechos humanos, incluido el derecho a la privacidad de las empresas de telecomunicaciones. Argentina es evaluada por la Asociación por los Derechos Civiles (ADC) desde 2018; Chile es evaluado por Derechos Digitales desde 2017; Colombia es evaluada por la Fundación Karisma desde 2015; Brasil es evaluado por InternetLab desde 2016; México es evaluado por R3D desde 2015; Perú es evaluado por Hiperderecho desde 2017; y Paraguay es evaluado por Tedic desde 2017. Ver, EFF, "¿Quién defiende tus datos", disponible en: https://www.eff.org/es/pages/quien-defiende-tus-datos, último acceso: 10 de abril de 2022.

[10] Diagnóstico regional que analiza la regulación de Argentina, Brasil, Chile, Colombia, Costa Rica, El Salvador, Guatemala, Honduras, México, Nicaragua, Paraguay, Perú, Estados Unidos y Uruguay. Recogido en, Rodríguez, *supra* nota 4.

[11] Cortés Castillo, Carlos, "Vigilancia de las comunicaciones en Colombia: el abismo entre la capacidad tecnológica y los controles legales", en: *Documentos Dejusticia*, N° 18, Bogotá, 2014, disponible en: https://www.dejusticia.org/publication/vigilancia-de-las-comunicaciones-en-colombia-el-abismo-entre-la-capacidad-tecnologica-y-los-controles-legales, último acceso: 10 de abril de 2022.

ción de las actividades de vigilancia de las telecomunicaciones e interceptación de las comunicaciones se materializó, según los diagnósticos por países, a través de leyes de interceptación, leyes de inteligencia y contrainteligencia, y reformas a los códigos penales o de procedimiento penal que buscaron legitimar prácticas o poderes existentes, sin fortalecer al tiempo los esfuerzos tendientes hacia la rendición de cuentas. En esta primera década los países que regularon así, fueron:

- A través de leyes de interceptación: El Salvador (decreto N° 285, 2010), Nicaragua (ley N° 735, 2010), Honduras (decreto ley N° 243, 2011), México (Ley Federal contra la Delincuencia Organizada, 2016).
- A través de leyes de inteligencia y contrainteligencia: Colombia (ley N° 1.621, 2013), Uruguay (ley N° 19.696, 2018), Paraguay (ley N° 524, 2014), Argentina (ley N° 27.126, 2015).
- A través de reformas a sus códigos penales o de procedimiento penal: Colombia (ley N° 1.453, 2011), Nicaragua (2014), México (Código de Procedimientos Penales, 2014; Ley Federal contra la Delincuencia Organizada, 2016).

Dichos informes también habían puesto de presente que en algunos países la normativa emanada por el Poder Ejecutivo, en aspectos como la retención de datos y la colaboración entre las empresas del sector de las telecomunicaciones y el sector público, se traducía en una evasión del debate público y democrático, y por supuesto, del debate judicial.[12] Este diagnóstico cerró con llamados a efectuar, en los años siguientes, procesos de reforma legislativa en línea con los estándares de derechos humanos, es decir, que unificaran los criterios para que la orden de limitación a la privacidad de las personas tuviera origen en una autoridad judicial, que la orden siguiera el debido proceso e integrara la valoración de un set específico de principios al analizar su procedencia (legalidad, objetivo legítimo, necesidad, proporcionalidad e idoneidad), y que contemplaran mejores mecanismos de protección de derechos y de supervisión de dichas actividades.

Por último, en esta primera década, la Relatoría Especial para la Libertad de Expresión de la Organización de Estados Americanos publicó dos informes hitos sobre el ejercicio de la libertad de expresión en internet, que recogieron estánda-

[12] En el balance conjunto sobre los diagnósticos de cada país, Katitza Rodríguez apunta que Colombia, Perú, Brasil, Honduras y Uruguay cuentan con decretos que provienen del Poder Ejecutivo que regulan actividades de retención de datos, así como dictaminan, en algunos casos, que la orden de vigilancia de las comunicaciones sea emitida por este último. Rodríguez, *supra* nota 4.

res sobre la protección de datos y la privacidad de cara a su ejercicio en línea, así como frente a la capacidad de vigilancia de las comunicaciones de los Estados. El primer informe de 2013 advirtió lo preocupante que era que los programas de vigilancia de las comunicaciones no estuvieran adecuados a los estándares en derechos humanos y los retos que proponen las nuevas tecnologías.[13] La interceptación, la retención de datos, la vigilancia masiva, entre otras actividades, debían tener un claro sustento legal orientado a criterios de proporcionalidad y necesidad para que su implementación fuera legítima. En el segundo informe de 2017, se reconoció que la vigilancia de las comunicaciones, incluida la que sucede en internet, en cualquiera de sus matices (vigilancia individualizada o masiva) constituía una injerencia en la vida privada de las personas y, que para ser ejercida de manera legítima, se debía contar con un marco legal transparente. Esto insistía, en definitiva, en que estuvieran en línea con los estándares del sistema interamericano.[14]

2. Final de la década

Hacia el final de la década es posible reconocer los avances legislativos en materia de protección de datos y privacidad frente a los retos advertidos, sin dejar de reconocer que todavía persisten deudas a ser resueltas.

2.1. Protección de datos

Entre los avances de la protección de datos, vale la pena apuntar al aumento del listado de países que, para el cierre de 2020, contaban con el reconocimiento constitucional del derecho a la protección de datos, así como con nuevas leyes generales o especiales de protección de datos ya sancionadas y otras más en curso. Al grupo de países con reconocimiento a nivel constitucional se habían integrado

[13] Comisión Interamericana de Derechos Humanos (Comisión IDH), "Libertad de expresión e internet", informe de la Relatoría Especial para la Libertad de Expresión, OEA/Ser.L/V/II, CIDH/RELE/INF.11/13, 31 diciembre 2013, § 147, disponible en: http://www.oas.org/es/cidh/expresion/docs/informes/2014_04_08_Internet_WEB.pdf, último acceso: 10 de abril de 2022.

[14] Comisión IDH, "Estándares para una internet libre, abierta e incluyente", informe de la Relatoría Especial para la Libertad de Expresión, OEA/Ser.L/V/II, CIDH/RELE/INF.17/17, 15 de marzo 2017, §§ 211 y 212, disponible en: http://www.oas.org/es/cidh/expresion/docs/publicaciones/internet_2016_esp.pdf, último acceso: 10 de abril de 2022.

México[15] (2014), Nicaragua[16] (2014), Chile (ley N° 21.096, 2018) y Cuba[17] (2019).

A nivel legislativo se habían sumado, con leyes sancionadas, Costa Rica (ley N° 8.968, 2011), El Salvador (decreto ley N° 695, 2011), Perú (ley N° 29.773, 2011), Nicaragua (ley N° 787, 2012), Colombia (ley N° 1.581, 2012), República Dominicana (ley N° 172, 2013), México (Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, 2017), Brasil (ley N° 13.709, 2018), Barbados (Data Protection Act, 2019), Panamá (ley N° 81, 2019), Paraguay (Ley de Protección de Datos Crediticios, ley N° 6.534, 2020) y Ecuador (Ley Orgánica de Protección de Datos, 2021), por mencionar tan solo algunos.

Se trata de progresos que, según Veridiana Alimonti y Katitza Rodríguez, dan cuenta de que la protección de datos no es más un fenómeno europeo.[18] La tendencia del reconocimiento del marco constitucional, no obstante, sigue sin proveer una mirada diferencial del tratamiento del derecho a la privacidad y del derecho a la protección de datos.[19]

Los retos, que informes y publicaciones recientes en materia de protección de datos apuntan hacia ellos –los cuales no se distancian de los del inicio de década–, reiteran, por ejemplo, la importancia de adoptar medidas para crear y fortalecer a las autoridades en protección de datos e insisten en la regulación de las dinámicas de transferencia y recolección transfronteriza de datos que sucede en internet y en la creación de mecanismos expeditos de protección, entre otros. También identifican nuevos retos como el reconocimiento del principio de minimización, el derecho a la portabilidad de los datos, el derecho a la revisión de las decisiones automatizadas sobre los individuos, la aplicación de dichas leyes a las actividades que desempeñan los Estados y sus autoridades,[20] y la actualización

[15] Constitución política de los Estados Unidos Mexicanos, capítulo I de los derechos humanos y sus garantías, art. 6, disponible en: https://mexico.justia.com/federales/constitucion-politica-de-los-estados-unidos-mexicanos/titulo-primero/capitulo-i/#articulo-6o, último acceso: 10 de abril de 2022.

[16] Constitución política de Nicaragua, capítulo I de derechos individuales, art. 26, disponible en: https://nicaragua.justia.com/nacionales/constitucion-politica-de-nicaragua/titulo-iv/capitulo-i/#articulo-26, último acceso: 10 de abril de 2022.

[17] Constitución de la República de Cuba., art. 97, disponible en: http://biblioteca.clacso.edu.ar/clacso/se/20191016105022/Constitucion-Cuba-2019.pdf, último acceso: 10 de abril de 2022.

[18] Rodríguez, Katitza y Alimonti, Veridiana, "Un panorama retrospectivo y futuro de la protección de datos en América Latina y España", EFF, 2020, disponible en: https://www.eff.org/es/deeplinks/2020/09/look-back-and-ahead-data-protection-latin-america-and-spain, último acceso: 10 de abril de 2022.

[19] Hernández Bauzá, Valentina, "Sucesos regulatorios en materias de privacidad e internet en América Latina, 2010-2020", Derechos Digitales América Latina, 2020, disponible en: https://www.derechosdigitales.org/wp-content/uploads/tendencias-privacidad-latam.pdf, último acceso: 10 de abril de 2022.

[20] Rodríguez y Alimonti, *supra* nota 18.

de la regulación para hacer frente al impacto de las nuevas tecnologías digitales, especialmente las biométricas, entre otras.

2.2. Privacidad

La continuidad de los informes por países de las organizaciones de la sociedad civil que responden a la pregunta "¿quién tiene mis datos?", que miden los compromisos de las empresas de telecomunicaciones y algunas plataformas de internet con la privacidad de sus suscriptores, junto con los informes que analizan la legislación sobre vigilancia de las comunicaciones, arrojan balances sobre progresos moderados. Sobre los compromisos de privacidad de las empresas de telecomunicaciones y de algunas plataformas de internet, se ha reconocido a fines de la década que la transparencia ya no es una excepción, sino una práctica mayormente extendida en los países evaluados. Sin embargo, el nivel de desagregación de la información de los reportes de transparencia varía en cada país, pese a que muchas empresas evaluadas operan a nivel regional.[21] Los reportes evidencian desafíos en la granularidad de la información asociada al tipo de datos que son retenidos, en la información sobre los procedimientos existentes para entregarlos y en su base legal. A la lucha por una mayor transparencia, se suman también los pedidos por integrar mecanismos de notificación a la persona afectada por dichas solicitudes, los cuales –según dichos informes– siguen siendo excepcionales.

Al cierre de la década, Nicaragua y Panamá se sumaron también a la lista de países evaluados en los informes de "¿Quién tiene mis datos?" con resultados que se asemejan a los primeros ejercicios de medición para otros países a mitad de la década anterior.[22] Por otro lado, la última versión del diagnóstico[23] del estado de la regulación de la vigilancia de las comunicaciones por países arroja conclusiones que insisten en los pedidos de la primera versión. Estas señalan que la regulación en buena parte de la región sigue siendo dispersa, lo que da pie a los

[21] Katitza, Rodríguez y Alimonti, Veridiana, "¿Quién defiende tus datos?: Four Years Setting the Bar for Privacy Protections in Latin America and Spain", EFF, 2019, disponible en: https://www.eff.org/deeplinks/2019/10/quien-defiende-tus-datos-four-years-setting-bar-privacy-protections-latin-america, último acceso: 10 de abril de 2022.

[22] Gullo, Karen, "IPANDETEC Releases First Report Rating Nicaragua Telecom Provider's Privacy Policies", EFF, 2020, disponible en: https://www.eff.org/deeplinks/2020/12/ipandetec-releases-first-report-rating-nicaraguan-telecom-providers-privacy, último acceso: 10 de abril de 2022; IPANDETEC Centroamérica, "¿Quien defiende tus datos? Nicaragua 2020", 2020, disponible en: https://www.ipandetec.org/2020/12/09/qdtd-nicaragua-2020, último acceso: 10 de abril de 2022.

[23] Este diagnóstico nuevamente analiza la regulación de Argentina, Brasil, Chile, Colombia, Costa Rica, El Salvador, Guatemala, Honduras, México, Nicaragua, Paraguay, Perú, Estados Unidos y Uruguay. Ver, Necesarios & Proporcionados, "Country Reports", disponible en: https://necessaryandproportionate.org/country-reports, último acceso: 10 de abril de 2022.

abusos, y que la amplia tipología sobre los datos que pueden ser solicitados por las autoridades (datos de las comunicaciones, metadatos, datos de los suscriptores, entre otros) sigue siendo confusa, lo que genera desequilibrios y vacíos en la protección a la privacidad de las personas.

Los avances, en este sentido, fueron advertidos en un informe reciente del Consorcio Al Sur[24] que reconoce la estandarización del requisito según el cual la limitación al secreto de las comunicaciones de las personas debe estar previsto en la ley. También, que existen, de manera casi unánime, en la región marcos regulatorios dedicados a las actividades de inteligencia e interceptación, y la consagración de límites asociados al respecto de las Constituciones y las leyes.

Los otros retos pendientes de la última década que siguen sin ser satisfechos, según Al Sur, tienen que ver con la actualización legislativa que pueda responder a las dinámicas de internet; al reconocimiento de las actividades y tecnologías digitales que facilitan la vigilancia masiva; a la regulación de la retención de datos de las personas usuarias de los servicios de telecomunicaciones; y al establecimiento de mecanismos para su protección efectiva, por citar tan solo algunos. Se enfatiza la necesidad de regular prácticas que no son tan nuevas, tales como el acceso directo, en el que las autoridades de investigación judicial y criminal pueden acceder a la infraestructura y a los datos de las telecomunicaciones y así suprimir de la ecuación a las empresas de telecomunicaciones, y la capacidad de llevar a cabo actividades de inteligencia en fuentes abiertas,[25] entre otras.

3. Algunas reflexiones

Los pedidos en torno a una mejor regulación en protección de datos y privacidad se encuentran mediados, en general, por un mayor respeto al principio de lega-

[24] El informe es un análisis comparativo del marco jurídico para la vigilancia de las comunicaciones de Argentina, Brasil, Chile, Colombia, México, Panamá, Paraguay y Perú. Ver, Rivera, Juan Camilo y Botero, Carolina, "Un marco jurídico de derechos humanos para la vigilancia de las comunicaciones en América Latina", Al Sur, 2021, pp. 7 y ss., disponible en: https://www.alsur.lat/reporte/un-marco-juridico-derechos-humanos-para-vigilancia-comunicaciones-en-america-latina, último acceso: 10 de abril de 2022.

[25] En este sentido, ver los informes que confirman la ausencia de regulación en esta materia, Ucciferri, Leandro, "Seguidores que no vemos: una primera aproximación al uso estatal del open-source intelligence (OSINT) y social media intelligence (SOCMINT)", ADC, 2018, disponible en: https://adc.org.ar/informes/seguidores-que-no-vemos, último acceso: 10 de abril de 2022; Céspedes Sagardía, Diandra y Machaca, Wilmer, "Ciberpatrullaje y desinformación durante la pandemia en Bolivia", Internet Bolivia, Derechos Digitales América Latina, 2021, disponible en: https://internetbolivia.org/publicacion/ciberpatrullaje-y-desinformacion-durante-la-pandemia-en-bolivia, último acceso: 10 de abril de 2022; Fundación para la Libertad de Prensa (FLIP), "El 'ciberpatrullaje' estatal es una estrategia de control que restringe libertades individuales y la expresión en línea", 2021, disponible en: https://flip.org.co/index.php/es/informacion/pronunciamientos/item/2726-el-ciberpatrullaje-estatal-es-una-estrategia-de-control-que-restringe-libertades-individuales-y-la-expresion-en-linea, último acceso: 10 de abril de 2022.

lidad, según el cual el ejercicio, así como la limitación a los derechos, debe estar regulado como fruto del debate público y democrático, y al principio de transparencia, que exige facilitar la búsqueda y entrega de información en la cantidad y detalle tal que permita el escrutinio de las personas en su calidad de ciudadanas o usuarias de servicios que son esenciales hoy en día para la comunicación de las personas. Cada tema, con sus prioridades, se encuentra unido no solo por el establecimiento de mayores y mejores garantías para la protección de la persona frente a la actuación del sector público y privado, sino por la creación de mecanismos de supervisión que puedan garantizar la protección de los derechos, lo que supone una garantía previa en torno a su autonomía e independencia.

Los retos en privacidad y protección de datos, con sus particularidades y tendencias, se encuentran mediados, además, por la existencia de internet y las nuevas tecnologías digitales que, al tiempo que amplifican los escenarios para el ejercicio de derechos también lo hacen para los de su limitación arbitraria o abusiva. En principio, una regulación capaz de responder a las necesidades que plantea cada una implica partir desde una base obvia, aunque no por ello común, como la adopción de los estándares en derechos humanos.

El trabajo de las diversas organizaciones de la sociedad civil, dedicadas a monitorear el estado de la regulación en cada tema al interior de sus países y de insistir en la adopción de dichos estándares, da cuenta de la lentitud con que se generan los cambios a nivel regulatorio en una región donde suceden en tiempos y con enfoques distintos. Este vistazo a lo que han sido las preocupaciones y progresos en la región durante la última década permite entender, para lo que sigue, los temas que aparecen (o deben aparecer) en el radar de proyectos de ley y leyes del Observatorio Legislativo en los últimos años. También permitirá trazar la agenda sobre metas satisfechas o todavía pendientes, que debieran poder ser mapeadas a futuro en la continuidad de este ejercicio de relevamiento de información legislativa.

IV. Marco normativo internacional

El Sistema Interamericano de Derechos Humanos (SIDH) a través de la Convención Americana sobre Derechos Humanos (CADH); la Declaración Americana de los Derechos y Deberes del Hombre (DADD); la jurisprudencia y opiniones consultivas proferidas por la Corte Interamericana de Derechos Humanos

(CIDH); así como los informes de casos, temáticos y por países, emitidos por la Comisión Interamericana de Derechos Humanos (CIDH) conforman, en su conjunto, el marco jurídico de base para la caracterización y análisis de los proyectos de ley y leyes en materia de privacidad y protección de datos. Todos los Estados sobre los que se orienta el trabajo del CELE hacen parte del SIDH.

1. Privacidad

1.1. Regulación

La regulación del derecho a la privacidad se encuentra prevista en el contenido del artículo 11 de la CADH (N° 2 y 3). La DADD, por su parte, prevé la protección a la privacidad de manera dispersa en distintas previsiones que pueden leerse en los artículos V, IX, y X. El artículo de la CADH señala que "nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación",[26] y "toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques".[27] Los artículos de la DADD señalan en su orden que "toda persona tiene derecho a la protección de la ley contra los ataques abusivos a su honra, a su reputación y a su vida privada y familiar",[28] "toda persona tiene el derecho a la inviolabilidad de su domicilio",[29] y "toda persona tiene derecho a la inviolabilidad y circulación de su correspondencia".[30] En la interpretación de la CADH, la Corte IDH ha expresado que el derecho a la privacidad provee a todas las personas de un ámbito inmune, reservado y exento a las injerencias, intervenciones o agresiones arbitrarias, abusivas o injustas de parte de las autoridades públicas y de terceros.[31]

El respeto a la privacidad es, así mismo, una precondición para el respeto a los otros derechos, como la libertad de expresión[32] –en línea y fuera de ella–, así

[26] Convención Americana sobre Derechos Humanos (CADH), art. 11, N° 2, 1969, disponible en: https://www.hchr.org.co/documentoseinformes/documentos/html/pactos/conv_americana_derechos_humanos.html, último acceso: 10 de abril de 2022.

[27] *Ibíd*., N° 3.

[28] OEA, Comisión IDH, "Declaración Americana de los Derechos y Deberes del Hombre", art. V, 1948, disponible en: https://www.oas.org/es/cidh/mandato/Basicos/declaracion.asp, último acceso: 10 de abril de 2022.

[29] *Ibíd*., art. IX.

[30] *Ibíd*., art. X.

[31] Corte Interamericana de Derechos Humanos (Corte IDH), "Fontevecchia y D'amico vs. Argentina", sentencia del 29 de noviembre de 2011, Fondo, Reparaciones y Costas, Serie C, N° 238, §§ 48 y ss., disponible en: https://www.corteidh.or.cr/CF/jurisprudencia2/ficha_tecnica.cfm?nId_Ficha=191, último acceso: 10 de abril de 2022.

32 Comisión IDH, *supra* nota 13, § 130.

como la ejercida por la niñez, la infancia y la adolescencia,[33] y por las mujeres periodistas;[34] la protesta social;[35] el debido proceso en casos relacionados a la investigación de delitos sexuales;[36] el reconocimiento de la identidad de género y el ejercicio del derecho a la autodeterminación personal;[37] el derecho a defender derechos especialmente cuando es ejercido por las mujeres;[38] entre otros. Y es un aspecto protegido, a su vez, por el ejercicio de otros derechos, como el de acceso a la información,[39] por ejemplo.

1.2. Ámbito de protección

El derecho a la privacidad protege, en concreto, a cuatro bienes jurídicos. El primero es el de contar con una esfera personal para la toma de decisiones libres sobre la propia vida. El segundo es tener un espacio de tranquilidad personal. El tercero es mantener reservados aspectos de la vida privada. Y el último es controlar la difusión de la información personal hacia terceros.[40]

En una verbalización un tanto diferente, la Comisión IDH se refirió a dichos bienes jurídicos así: el primero está destinado a permitir una esfera personal resistente a las injerencias arbitrarias del tercero y de terceras personas. El segundo

---

[33] Comisión IDH, "Niñez, libertad de expresión y medios de comunicación en las Américas", informe de la Relatoría Especial para la Libertad de Expresión, OEA/Ser.L/V/II, CIDH/RELE/INF.23/19, febrero 2019, §§ 3, 82, 114, disponible en: http://www.oas.org/es/cidh/expresion/informes/Nin%CC%83ezLEXMediosESP.pdf, último acceso: 10 de abril de 2022.

[34] Comisión IDH, "Mujeres periodistas y libertad de expresión", informe de la Relatoría Especial para la Libertad de Expresión, OEA/Ser. L/V/II, CIDH/RELE/INF.20/18, 31 de octubre 2018, § 140, disponible en: http://www.oas.org/es/cidh/expresion/docs/informes/MujeresPeriodistas.pdf, último acceso: 10 de abril de 2022.

[35] Comisión IDH, "Protesta y derechos humanos", informe de la Relatoría Especial para la Libertad de Expresión, OEA/Ser.L/V/II, CIDH/RELE/INF.22/19, septiembre 2019, § 299, disponible en: https://www.oas.org/es/cidh/expresion/publicaciones/ProtestayDerechosHumanos.pdf, último acceso: 10 de abril de 2022.

[36] Comisión IDH, "Estándares jurídicos vinculados a la igualdad de género y a los derechos de las mujeres en el Sistema Interamericano de Derechos Humanos: desarrollo y aplicación", OEA/Ser. L/V/II.143, doc. 60, 3 de noviembre 2011, § 78, disponible en: https://www.oas.org/es/cidh/mujeres/docs/pdf/ESTANDARES%20JURIDICOS.pdf, último acceso: 10 de abril de 2022.

[37] Comisión IDH, "Informe sobre personas trans y de género diverso y sus derechos económicos, sociales, culturales y ambientales", informe para la Relatoría Especial sobre los Derechos Económicos, Sociales, Culturales, OEA/Ser.L/V/II, doc. 239, 7 de agosto 2020, §§ 36 y 67, disponible en: https://www.oas.org/es/cidh/informes/pdfs/PersonasTransDESCA-es.pdf, último acceso: 10 de abril de 2022.

[38] Comisión IDH, "Violencia y discriminación contra mujeres, niñas y adolescentes: buenas prácticas y desafíos en América Latina y el Caribe", OEA/Ser.L/V/II, doc. 233, 14 de noviembre 2019, § 129, disponible en: http://www.oas.org/es/cidh/informes/pdfs/ViolenciaMujeresNNA.pdf, último acceso: 10 de abril de 2022.

[39] Comisión IDH, "El derecho de acceso a la información en el marco jurídico interamericano", informe para la Relatoría Especial para la Libertad de Expresión, OEA/Ser.L/V/II, CIDH/RELE/INF.1/09, § 56, disponible en: http://www.oas.org/es/cidh/expresion/docs/cd/sistema_interamericano_de_derechos_humanos/index_DAIMJI.html, último acceso: 10 de abril de 2022.

[40] Corte IDH, "Fontevecchia y D'amico vs. Argentina", *supra* nota 31, §§ 48 y 91.

está dirigido a permitir el gobierno propio, en soledad, según el proyecto de vida personal. El tercero está enfocado en el secreto de todos los datos que se producen en dicho espacio reservado y cuya divulgación y circulación se encuentran restringidas cuando no media el consentimiento de la persona. Y el cuatro faculta a la persona a la protección de la propia imagen para que esta no sea utilizada sin consentimiento del titular.[41]

El ámbito de protección normativa de la privacidad se extiende sobre el domicilio, la correspondencia y la vida familiar y privada que, en criterio de la Corte IDH, "se encuentran intrínsecamente ligados, ya que el domicilio se convierte en un espacio en el cual se puede desarrollar libremente la vida familiar y privada".[42] El principio de protección gira en torno a su inviolabilidad, salvo que medie el consentimiento de la persona o exista orden judicial que justifique la injerencia o la intromisión.

La expresión "domicilio" gira en torno al espacio de desarrollo familiar y personal del individuo sin importar si este tiene carácter personal o laboral. Por "correspondencia" se entienden comprendidas, a su turno, las comunicaciones telefónicas, las que transcurren por internet[43] y a través de las nuevas tecnologías. Incluye tanto a los datos sobre el contenido de las comunicaciones, como a los datos que identifican a las comunicaciones o datos propios "del proceso de comunicación" o metadatos.[44] La "vida privada" es "un concepto amplio que no es susceptible de definiciones exhaustivas",[45] que comprende aspectos sobre la identidad física, sexual, de género, emocional y social de la persona,[46] la forma en cómo la persona se ve a sí misma, cómo y cuándo decide proyectarla a los de-

---

41 Comisión IDH, *supra* nota 13, § 131.

42 Corte IDH, "Escué Zapata vs. Colombia", sentencia del 5 de mayo de 2008, Fondo, Reparaciones y Costas, Serie C, N° 178, § 95, disponible en: https://www.corteidh.or.cr/CF/jurisprudencia2/ficha_tecnica.cfm?nId_Ficha=227, último acceso: 10 de abril de 2022.

43 Corte IDH, "Tristán Donoso vs. Panamá", sentencia del 27 de enero de 2009, Excepciones Preliminares, Fondo, Reparaciones y Costas, Serie C, N° 193, § 55, disponible en: https://www.corteidh.or.cr/CF/jurisprudencia2/ficha_tecnica.cfm?nId_Ficha=253, último acceso: 10 de abril de 2022.

44 Corte IDH, "Escher y otros vs. Brasil", sentencia del 20 de noviembre de 2009, Excepciones Preliminares, Fondo, Reparaciones y Costas, Serie C, N° 208, § 114, disponible en: https://www.corteidh.or.cr/cf/jurisprudencia2/ficha_tecnica.cfm?nId_Ficha=277&lang=es, último acceso: 10 de abril de 2022.

45 Corte IDH, "Atala Riffo y Niñas vs. Chile", sentencia del 21 de noviembre de 2012, Fondo, Reparaciones y Costas, Serie C, N° 254, § 162, disponible en: https://www.corteidh.or.cr/cf/Jurisprudencia2/ficha_tecnica.cfm?nId_Ficha=196, último acceso: 10 de abril de 2022.

46 Corte IDH, "Artavia Murillo y otros (fertilización in vitro) vs. Costa Rica", sentencia del 28 de noviembre de 2012, Excepciones Preliminares, Fondo, Reparaciones y Costas, Serie C, N° 257, § 143, disponible en: https://www.corteidh.or.cr/cf/Jurisprudencia2/ficha_tecnica.cfm?nId_Ficha=235, último acceso: 10 de abril de 2022.

más. Por "vida familiar" se incluye la decisión sobre el derecho a conformar una familia y sobre la autonomía reproductiva, entre otros.[47]

1.3. Estándares para su limitación

Las limitaciones a la privacidad, sean directas o indirectas,[48] no deben inhibir ni restringir la investigación y la difusión de información de interés público ni la expresión y la opinión de las personas.[49] Su garantía, en conexión con la libertad de expresión, debe poder ser llevada a cabo a través de la protección del anonimato y la protección de datos.[50] Su limitación se somete, en todo caso, al test tripartito. Para que las limitaciones al derecho a la privacidad ejercidas por el Estado o por particulares sean legítimas, se debe satisfacer el test tripartito de legalidad, necesidad y proporcionalidad.

El "principio de legalidad" significa la expedición de leyes en sentido formal y material, fruto de la deliberación democrática y en atención al procedimiento legislativo que debe surtir el órgano legislativo, el cual tiene que definir "de manera expresa, taxativa, precisa y clara"[51] las reglas según las cuales procede dicha limitación, su duración, los organismos competentes para expedir las órdenes que limitan el derecho a la privacidad, los organismos encargados de implementarlas y supervisarlas, entre otros. Dichas limitaciones deben perseguir, a su vez, un objetivo imperioso, compatible con la CADH, que puedan orbitar en torno a la protección de la seguridad nacional, la protección de la moral pública y de derechos de terceros. La interpretación del concepto de seguridad nacional tiene que hacerse al atender las "justas exigencias del bien común en una sociedad democrática"[52] y debe tener un carácter excepcional. Si la protección de los objetivos imperiosos, especialmente el de seguridad nacional, lleva a justificar el monitoreo o la interceptación de las comunicaciones, la ley deberá establecer la necesidad de una orden judicial.

---

[47] *Ibíd*., § 150.

[48] Comisión IDH, *supra* nota 13, § 150.

[49] Comisión IDH, "Declaración de principios sobre libertad de expresión", N° 10, disponible en: https://www.cidh.oas.org/basicos/declaracion.htm, último acceso: 10 de abril de 2022.

[50] Comisión IDH, *supra* nota 13, § 133.

[51] Comisión IDH, *supra* nota 14, § 217.

[52] Comisión IDH, "Derecho a la información y seguridad nacional", informe para la Relatoría Especial para la Libertad de Expresión, OEA/Ser.L/V/II, CIDH/RELE/INF.24/20, julio 2020, § 76, disponible en: http://www.oas.org/es/cidh/expresion/informes/DerechoInformacionSeguridadNacional.pdf, último acceso: 10 de abril de 2022.

El "principio de necesidad" apunta a que las limitaciones respondan a una necesidad cierta e imperiosa para el logro de los objetivos legítimos propuestos, y acarrea un juicio estricto para evaluar la existencia de medios menos restrictivos para el ejercicio de derechos.[53] El "principio de proporcionalidad" implica el análisis del impacto de la medida en el ejercicio de otros derechos. Al tratarse de la limitación de la privacidad en internet, el análisis de proporcionalidad debe considerar la arquitectura y los principios de la Red Iberoamericana de Protección de Datos.[54]

Los "Principios internacionales sobre la aplicación de los derechos humanos a la vigilancia de las comunicaciones"[55] prevén, en materia de necesidad, la carga argumentativa que existe en hombros del Estado para justificar una limitación a la privacidad. Y en relación a la proporcionalidad, apuntan al establecimiento de una autoridad judicial competente que pueda analizar el grado de probabilidad de comisión de delitos o de amenazas en contra del objetivo legítimo que se quiere proteger a través de la limitación a la privacidad, la ausencia de técnicas menos invasivas o que, al serlo, resultan fútiles para la protección del objetivo legítimo, entre otros.

1.4. Obligaciones para los Estados

Los Estados que limiten el derecho a la privacidad se encuentran en el deber de aplicar el principio de máxima divulgación en materia de acceso a la información[56] en torno a tres aspectos: i) las políticas y prácticas de vigilancia de las comunicaciones; ii) la adquisición, el desarrollo, la actualización de los sistemas dirigidos a dichas actividades, los protocolos y las autoridades facultadas para su uso, las condiciones para su autorización, la supervisión y la implementación; y iii) las estadísticas respecto al número de solicitudes de interceptación y solicitud de los datos de las comunicaciones de las personas, las que fueron aprobadas y rechazadas, el tipo de investigación en el marco en el cual se solicitan, su duración, las solicitudes según tipo de proveedor, entre otros.[57] Tienen, además, la

[53] Comisión IDH, *supra* nota 13 § 160.

[54] Comisión IDH, *supra* nota 14, § 222.

[55] Necesarios & Proporcionados, *supra* nota 23.

[56] OEA, Comisión IDH, "Declaración conjunta sobre programas de vigilancia y su impacto en la libertad de expresión", Relator Especial de las Naciones Unidas (ONU) para la Protección y Promoción del Derecho a la Libertad de Opinión y de Expresión y Relatora Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos de la OEA, N° 12 y ss., 2013, disponible en: https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=926&lID=2, último acceso: 11 de abril de 2022.

[57] Comisión IDH, *supra* nota 14, §§ 218 y 225; Comisión IDH, *supra* nota 13, § 168.

obligación de implementar el principio de transparencia activa en la divulgación de información sobre abusos a las facultades de vigilancia o el despliegue de sistemas ilegales de vigilancia de las comunicaciones privadas.[58]

Asimismo, les cabe la obligación de proveer garantías procedimentales para proteger y asegurar el derecho a la privacidad en los casos en que se precise su limitación. En ese sentido, la limitación debe ser materializada a través de una orden judicial previa,[59] la cual tiene que "estar debidamente fundada"[60] y ser respetuosa del debido proceso,[61] debe ser proferida por una autoridad judicial independiente, especializada y competente[62] para tomar decisiones sobre la legalidad de la medida.[63]

En ese mismo sentido, los Estados deben establecer mecanismos de supervisión independientes y efectivos sobre "las autoridades encargadas de realizar las tareas de vigilancia", que puedan "asegurar la transparencia, cuando proceda, y la rendición de cuentas por las actividades de vigilancia de las comunicaciones y la interceptación (…) que realice el Estado".[64] Deben abstenerse de debilitar los mecanismos existentes de seguridad digital[65] y, según se advirtió más recientemente, tienen el deber de asegurar que los desarrollos tecnológicos respeten la privacidad desde el diseño.[66]

---

[58] OEA, Comisión IDH, *supra* nota 56, N° 14.

[59] Comisión IDH, *supra* nota 14, § 217.

[60] *Ibíd*., § 223.

[61] Comisión IDH, *supra* nota 49, N° 9.

[62] Comisión IDH, *supra* nota 13, § 165.

[63] Comisión IDH, "Informe sobre terrorismo y derechos humanos", OEA/Ser.L/V/II.116, doc. 5 rev. 1 corr., 22 octubre 2002, § 371, disponible en: http://www.cidh.org/Terrorism/Span/indice.htm, último acceso: 11 de abril de 2022.

[64] Comisión IDH, *supra* nota 13, § 170; OEA, Comisión IDH, *supra* nota 56, N° 12.

[65] OEA, Comisión IDH, "Declaración conjunta sobre la libertad de expresión y el combate del extremismo violento", el Relator Especial de las Naciones Unidas (ONU) para la Libertad de Opinión y de Expresión, la Representante para la Libertad de los Medios de Comunicación de la Organización para la Seguridad y la Cooperación en Europa (OSCE), el Relator Especial de la Organización de Estados Americanos (OEA) para la Libertad de Expresión y la Relatora Especial sobre Libertad de Expresión y Acceso a la Información de la Comisión Africana de Derechos Humanos y de los Pueblos (CADHP), num. 2, lit. j, 2016, § ii, disponible en: https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=1022&lID=2, último acceso: 11 de abril de 2022.

[66] OEA, Comisión IDH, "Declaración conjunta del vigésimo aniversario: desafíos para la libertad de expresión en la próxima década", el Relator Especial de las Naciones Unidas (ONU) para la Libertad de Opinión y de Expresión, el Representante de la Organización para la Seguridad y la Cooperación en Europa (OSCE) para la Libertad de los Medios de Comunicación, el Relator Especial de la Organización de Estados Americanos (OEA) para la Libertad de Expresión y la Relatora Especial sobre Libertad de Expresión y Acceso a la Información de la Comisión Africana de Derechos Humanos y de los Pueblos (CADHP), num. 2, lit. f, 2019, disponible en: https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=1146&lID=2, último acceso: 11 de abril de 2022.

2. Protección de datos

El derecho a la protección de datos es una forma de garantía del derecho a la privacidad.[67] Es uno de los bienes protegidos por este derecho que reconoce la facultad de controlar la difusión de la información personal hacia terceros –información que puede identificar o que hace identificable a una persona, y de cuya creación, almacenamiento y procesamiento depende el funcionamiento de internet–.[68] Se ejerce a través de la acción de habeas data que tiene un carácter fiscalizador y sirve no solo para materializar judicialmente la facultad de control sobre la propia información, sino para repeler las acciones de recopilación excesiva o injustificada de la información personal que llevan a cabo los Estados.[69]

2.1. Ámbito de protección

Sobre el derecho a la protección de datos, la "Declaración de principios sobre libertad de expresión" señaló que "toda persona tiene el derecho a acceder a la información sobre sí misma o sus bienes en forma expedita y no onerosa, ya esté contenida en bases de datos, registros públicos o privados y, en el caso de que fuere necesario, actualizarla, rectificarla y/o enmendarla".[70] El ejercicio del derecho a la protección de datos debe suceder con una base legal que justifique el tratamiento, en atención al principio de legalidad del test tripartito. Cuando la autorización al tratamiento se justifique en el consentimiento de la persona, este deberá ser libre e informado para ser válido. Cuando el encargado del tratamiento sea el Estado, se deben fijar controles para que los datos sean utilizados para los fines advertidos, su tratamiento se extienda sólo durante el tiempo consentido, y sean compartidos solo con los terceros y en las condiciones y con los fines informados y consentidos por su titular.[71]

El tratamiento de datos biométricos se debe ajustar de manera estricta al test tripartito. Los eventos sobre su limitación deben estar contemplados en la ley y ser sometidos a control administrativo y judicial.[72]

---

67 Naciones Unidas (ONU), Asamblea General, "Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Frank La Rue", A/HRC/17/27, 16 mayo 2011, § 58, disponible en: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G11/132/01/PDF/G1113201.pdf?OpenElement, último acceso: 11 de abril de 2022.

68 Comisión IDH, *supra* nota 14, §§ 203 y 204.

69 OEA, Comisión IDH, "Antecedentes e interpretación de la Declaración de Principios sobre Libertad de Expresión", disponible en: https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=132&lID=2, último acceso: 11 de abril de 2022.

70 Comisión IDH, *supra* nota 49, N° 3.

71 Comisión IDH, *supra* nota 14, § 206.

72 *Ibíd*., § 209.

Desde 2015, el Comité Jurídico Interamericano (CJI) de la Organización de Estados Americanos adoptó los "Principios interamericanos sobre privacidad y protección de datos".[73] Su objetivo es el de instar a los Estados a adoptar medidas legislativas en dicha materia, en atención a una propuesta marco compatible con los estándares del SIDH que pueda reflejar algunos de los estándares ya desarrollados en ese sentido. Su contenido busca responder al contexto regulatorio de la región y a sus adelantos tecnológicos.[74] Pese a que algunas organizaciones de la sociedad civil[75] advierten que se trata de estándares de menor calado en comparación con otros, como los de la Organización para la Cooperación y Desarrollo Económico (OCDE),[76] la Unión Europea[77] y Asia-Pacífico,[78] los principios del CJI reconocen en su más reciente versión[79] trece principios que acogen, en parte, los desarrollos de aquellos otros.

Los principios interamericanos se refieren a las finalidades legítimas y de lealtad; al principio de transparencia y consentimiento; al de pertinencia y necesidad; al de tratamiento y conservación limitados; al de confidencialidad; al de seguridad de los datos; al de exactitud de los datos; al derecho de acceso, rectificación, cancelación y oposición (ARCO), y derecho a la portabilidad; al principio de protección de los datos personales sensibles; al de responsabilidad; al flujo transfronteri-

[73] "En el mes de marzo de 2012, el CJI adoptó una 'Propuesta de Declaración de Principios de Privacidad y Protección de Datos Personales en las Américas' cuyo fin primordial fue orientar a los Estados miembros de la OEA a adoptar medidas en respeto a la privacidad". Dicha propuesta fue luego adoptada en 2015 bajo el título "Guía legislativa sobre la protección de datos en las Américas". Ver, OEA, CJI, "Guía legislativa sobre la privacidad y la protección de datos personales en las Américas", 2015, disponible en: http://www.oas.org/es/sla/ddi/docs/proteccion_datos_personales_Guia_Legilsativa_CJI.pdf, último acceso: 10 de abril de 2022.

[74] OEA, "La privacidad y la protección de datos personales", informe presentado por la doctora Ana Elizabeth Villalta Vizcarra al Comité Jurídico Interamericano, CJI/doc.541/17 corr.1, 2017, p. 1, disponible en: http://www.oas.org/es/sla/cji/docs/informes_culminados_recientemente_Proteccion_Datos_Personales_CJI-doc_541-17_corr1.pdf, último acceso: 11 de abril de 2022.

[75] Por ejemplo, ADC en su informe señala que "si bien dichos principios pretenden guiar el desarrollo de los sistemas legales de protección de datos personales de los países que integran la OEA, que obviamente incluye a los países de Latinoamérica, cabe decir que los mismos no fueron tenidos como referencia de estándares internacionales para la comparación que aquí se pretende realizar. Ello así toda vez que los principios adoptados por el Comité Jurídico establecen una línea muy baja de protección, quedando por debajo de los sistemas vigentes en varios países de la región y muy lejanos de los estándares de protección de datos personales propiciado por el sistema europeo", Ucciferri, *supra* nota 5, p. 16.

[76] Organización para la Cooperación y Desarrollo Económico (OCDE), "Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales" de 1980 y su actualización de 2013, disponible en: https://www.oecd.org/sti/ieconomy/15590267.pdf, último acceso: 11 de abril de 2022.

[77] Consagrados en la directiva 95/46/CE, hoy derogada por el Reglamento General de Protección de Datos.

[78] Marco de Privacidad para la Organización Internacional de Cooperación Económica de Asia-Pacífico (APEC, por sus siglas en inglés) de 2005 y su actualización de 2015.

[79] OEA, CJI, "Principios actualizados del Comité Jurídico Interamericano sobre la privacidad y la protección de datos personales, con anotaciones", OEA/Ser.Q, CJI/doc. 638/21, 8 abril 2021, disponible en: http://www.oas.org/es/sla/cji/docs/CJI-doc_638-21.pdf, último acceso: 11 de abril de 2022.

zo de datos y responsabilidad; a las excepciones en su aplicación; y uno dedicado finalmente a la creación de autoridades de protección de datos independientes. Aquellos principios están dirigidos al responsable, bien se encuentre en cabeza del sector público o bien del sector privado, en las actividades de tratamiento de los datos personales que identifican o hacen identificable a una persona.

2.2. Obligaciones de los Estados

Los Estados tienen el deber de: i) adoptar políticas para prohibir el tratamiento de datos, que sean incompatibles con los derechos humanos; ii) prohibir el almacenamiento, el análisis y la divulgación, salvo que exista base legal o la persona haya consentido para autorizar su tratamiento; iii) establecer mecanismos de supervisión y control efectivos e independientes;[80] iv) crear mecanismos y procedimientos para cuestionar el tratamiento de datos, y establecer una autoridad competente para resolver solicitudes de ese tipo;[81] y v) investigar los abusos a los derechos humanos producto del tratamiento indebido de los datos biométricos.[82]

V. Análisis regional

En este análisis regional se busca identificar, a partir de los criterios de caracterización general[83] de los proyectos, las tendencias a nivel regional en materia de privacidad y protección de datos. De entrada, se advierte que el balance de preocupaciones de la última década, que se abordó antes, todavía no encuentra pleno eco en la actividad legislativa de los nueve países objeto de revisión, en los últimos años.

---

[80] Comisión IDH, *supra* nota 14, § 205.

[81] *Ibíd*., § 208.

[82] *Ibíd*., § 29.

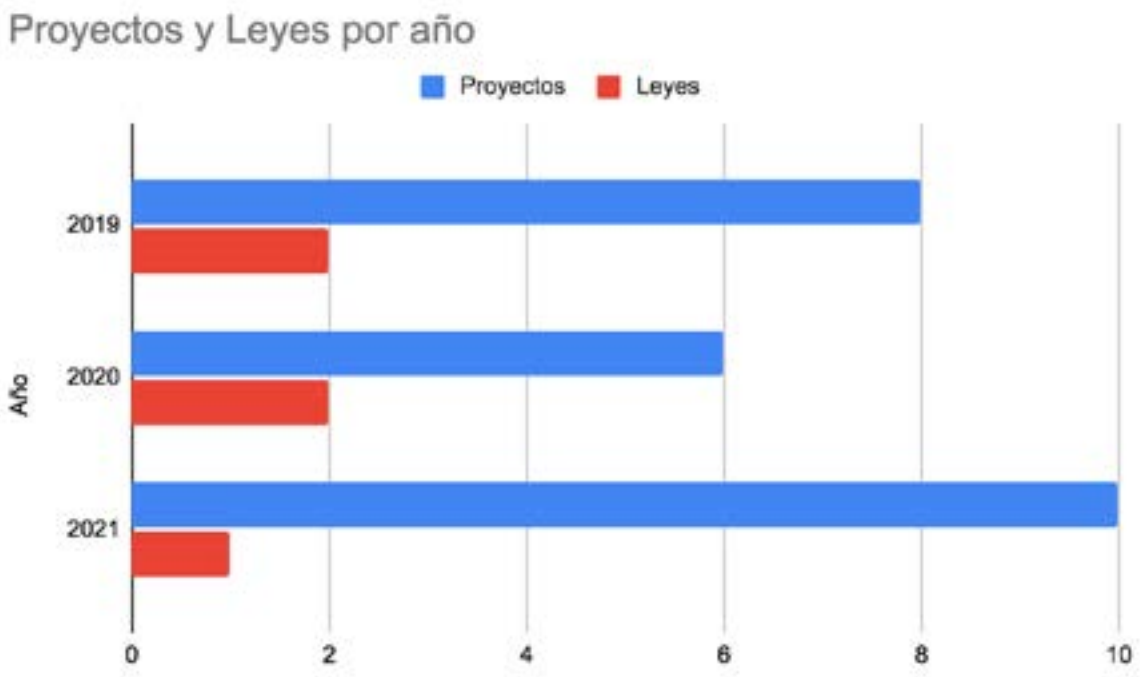
[83] Algunos de los criterios generales de caracterización en privacidad a los que acudimos para esta sección fueron: país (Argentina, Brasil, Chile, Colombia, Ecuador, Guatemala, México, Paraguay y Perú); tipo de iniciativa (proyecto de ley, ley); origen (Senado, Cámara, Cámara Única); fecha (año); y tema (regulación de la vigilancia individualizada de las comunicaciones, regulación de la vigilancia masiva de las comunicaciones, regulación de la privacidad de niños, niñas y adolescentes, regulación de la privacidad en el ejercicio de otros derechos).

Algunos de los criterios generales de caracterización en protección de datos a los que acudimos para esta sección fueron: país (Argentina, Brasil, Chile, Colombia, Ecuador, Guatemala, México, Paraguay y Perú); tipo de iniciativa (proyecto de ley, ley); origen (Senado, Cámara, Cámara Única); fecha (año); tipo de régimen (general, especial); y tema (agrupados en iniciativas sobre generalidades en el tratamiento de la protección de datos; iniciativas sobre el tratamiento de datos por sector, actividad y responsable; iniciativas sobre el tratamiento según tipos de titulares y tipos de datos; iniciativas sobre el tratamiento de datos ejercido en internet y a través de otras tecnologías digitales; iniciativas sobre el tratamiento de datos con ocasión de la pandemia; e iniciativas "otras").

1. Privacidad

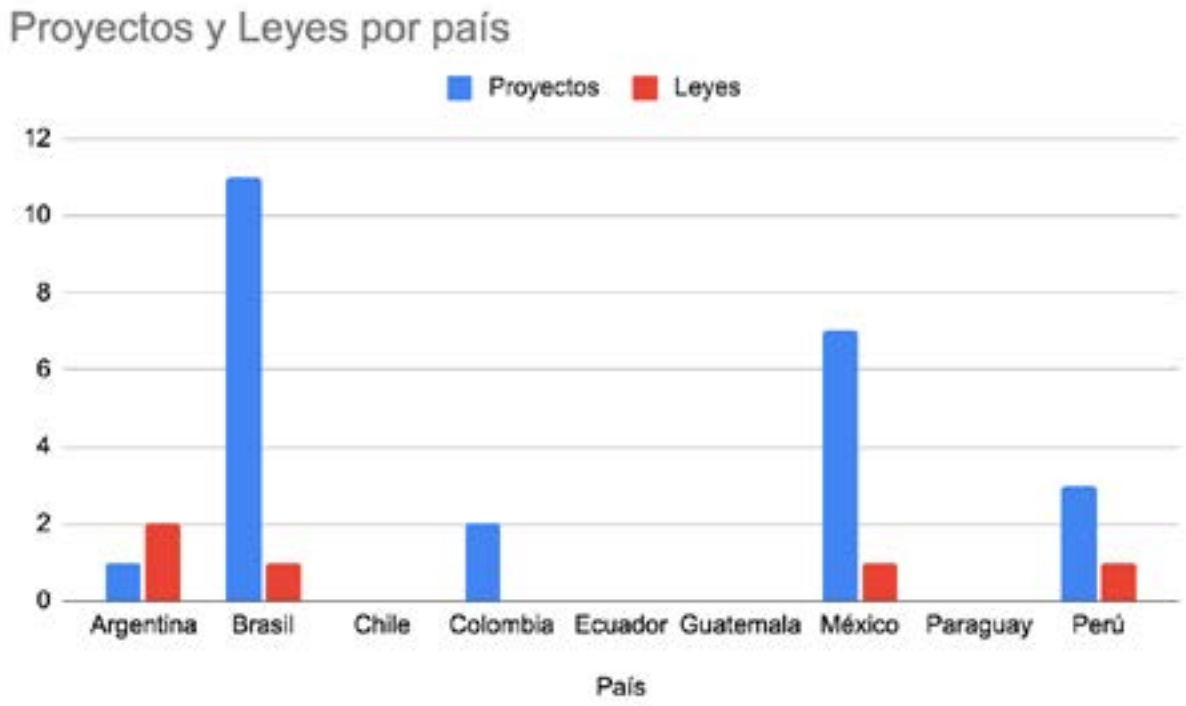
1.1. Balance general

Desde el 1° de enero de 2019 y hasta el 30 de septiembre de 2021, se tramitó –en los nueve países objeto de revisión– un total de 24 proyectos de ley (82,8%) y 5 leyes (17,2%) en privacidad.[84] En 2019, se tramitó un total de 8 proyectos de ley y 2 leyes; en 2020, se dio curso a 6 proyectos de ley y 3 leyes; y, en 2021, se han presentado 9 proyectos de ley y 1 ley. El último año ha sido el más activo para los países analizados.



Los datos según nivel de actividad legislativa son los siguientes: Argentina (1 proyecto de ley, 2 leyes); Brasil (11 proyectos de ley, 1 ley); Colombia (2 proyectos de ley, 0 leyes); México (7 proyectos de ley, 1 ley); Perú (3 proyectos de ley, 1 ley); en Chile, Ecuador, Guatemala y Paraguay no se hallaron proyectos de ley ni leyes. El país más activo en la materia es Brasil, seguido de México y Perú.

[84] De acuerdo con lo advertido en la introducción, se incluyeron proyectos de ley que refieren en su título al derecho a la privacidad, otros que por su contenido integran previsiones que impactan en el ejercicio de este derecho. Se integraron proyectos de ley y leyes que referían al impacto en el derecho a la privacidad en línea y fuera de ella.



Se clasificaron los proyectos según autoridad de origen en Senado, Cámara o Cámara Única (como sucede en Perú, Ecuador y Guatemala). Los datos desagregados son los siguientes: Senado (10 proyectos de ley, 4 leyes); Cámara de Representantes o de Diputados (11 proyectos de ley, 0 leyes); y Cámara Única (3 proyectos de ley, 1 ley).

Por temas, los agrupamos en cinco grupos. Grupo de iniciativas sobre vigilancia individualizada de las comunicaciones; grupo de iniciativas sobre la vigilancia masiva de las comunicaciones; iniciativas que regulan la privacidad de niños, niñas y adolescentes; iniciativas que regulan el ejercicio y protección de la privacidad y otros derechos; y el grupo "otros".

1. Grupo de iniciativas sobre vigilancia individualizada de las comunicaciones

En este grupo, se clasificaron los proyectos de ley y leyes sobre la interceptación de las comunicaciones de personas involucradas en procesos penales, la solicitud y el acceso directo a los datos del suscriptor de servicios de telecomunicaciones en investigaciones delictivas, y el acceso a los sistemas de cámaras de videovigilancia privada y pública para la investigación de delitos contra la seguridad ciudadana. En este grupo, se presentaron un total de 16 proyectos de ley y 3 leyes.

2. Grupo de iniciativas sobre vigilancia masiva de las comunicaciones

En este grupo, se clasificaron los proyectos de ley y leyes en la región que han abordado el monitoreo del espectro electromagnético. Si bien se reconoce que son mucho más diversas las actividades comprendidas en la facultad de vigilancia masiva que ejercitan algunos Estados sobre su población, la actividad legislativa desde 2019 a la fecha es más bien escasa en dicha materia, pese a que en la región se han documentado[85] diversos casos de abuso de este tipo de facultad. Dicho esto, se caracterizaron solo 3 proyectos de ley y ninguna ley.

3. Grupo de iniciativas sobre protección de la privacidad de niños, niñas y adolescentes

Se clasificaron como iniciativas en materia de privacidad los proyectos de ley y leyes que tienen que ver con la investigación penal de los eventos de recolección y difusión no consentida de los datos personales de niños, niñas y adolescentes.

Esta clasificación tuvo lugar en este tema y no en el de protección de datos porque se trata de hechos frente a los que las legislaciones pueden: i) no proveer garantías en torno al ejercicio de las facultades de acceso, rectificación, oposición o cancelación de los datos frente a terceros; o ii) en caso de proveerlas, su ejercicio puede no resultar comprehensivo de otros bienes jurídicos que pueden resultar afectados, como el derecho a la autonomía, a la salud mental y al bienestar físico, entre otros.[86] En este grupo, se identificaron 1 proyecto de ley y 1 ley.

4. Grupo de iniciativas sobre protección de la privacidad en el ejercicio de otros derechos

Se clasificaron así a los proyectos de ley (2) y leyes (1) que consagran como delito

---

[85] San Martín, María, "#GobiernoEspía: vigilancia masiva del gobierno mexicano hacia defensores/as y organizaciones de derechos humanos", Front Line Defenders, 2017, disponible en: https://www.frontlinedefenders.org/es/blog/post/gobiernoespia-widespread-mexican-government-surveillance-human-rights-defenders-and, último acceso: 13 de abril de 2022; Fundación Karisma, "Sistemas de vigilancia en Colombia al descubierto", 2015, disponible en: https://web.karisma.org.co/sistemas-de-vigilancia-en-colombia-al-descubierto, último acceso: 13 de abril de 2022.

[86] Al respecto, tomamos en consideración el informe "La inteligencia artificial y la privacidad, así como la privacidad de los niños" del Relator Especial sobre el derecho a la privacidad de las Naciones Unidas, Josehp A. Cannataci. En dicho informe, se reconoce la titularidad del derecho a la privacidad de los niños (toda persona menor de 18 años –ver, § 76–), y se pone de presente que la lógica en el tratamiento de su información, orientada por la protección de datos, puede requerir acciones más allá de las que facultan a la actualización, a la rectificación, a la cancelación y a la oposición cuando se trata, por ejemplo, de conductas que atentan contra la libertad y la autonomía del menor. Ver, ONU, Asamblea General, "La inteligencia artificial y la privacidad, así como la privacidad de los niños", informe del Relator Especial sobre el derecho a la privacidad, Joseph A. Cannataci, A/HRC/46/37, 25 de enero 2021, disponible en: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G21/015/68/PDF/G2101568.pdf?OpenElement, último acceso: 13 de abril de 2022.

la difusión no consentida de imágenes con contenido sexual.

Se caracterizaron como iniciativas en materia de privacidad en tanto que la protección de datos no responde de manera plena a las expectativas de protección y amparo para la víctima que generan estos eventos pues: i) colocan al victimario en la situación del "responsable de datos", siendo que no lo es; y ii) los mecanismos de protección de datos resultan insuficientes, pues no tienen una vocación de reparación integral a otros bienes jurídicos protegidos que pueden resultar afectados como la autonomía o la libertad sexual de la persona.[87]

5. Grupo "otros"

Se clasificaron aquí los proyectos de ley sobre creación de bases de datos o registros de agresores sexuales, pues ordena el establecimiento de registros con su información personal en los cuales no se reconoce su ejercicio al derecho a controlar su información.[88]

2. Protección de datos

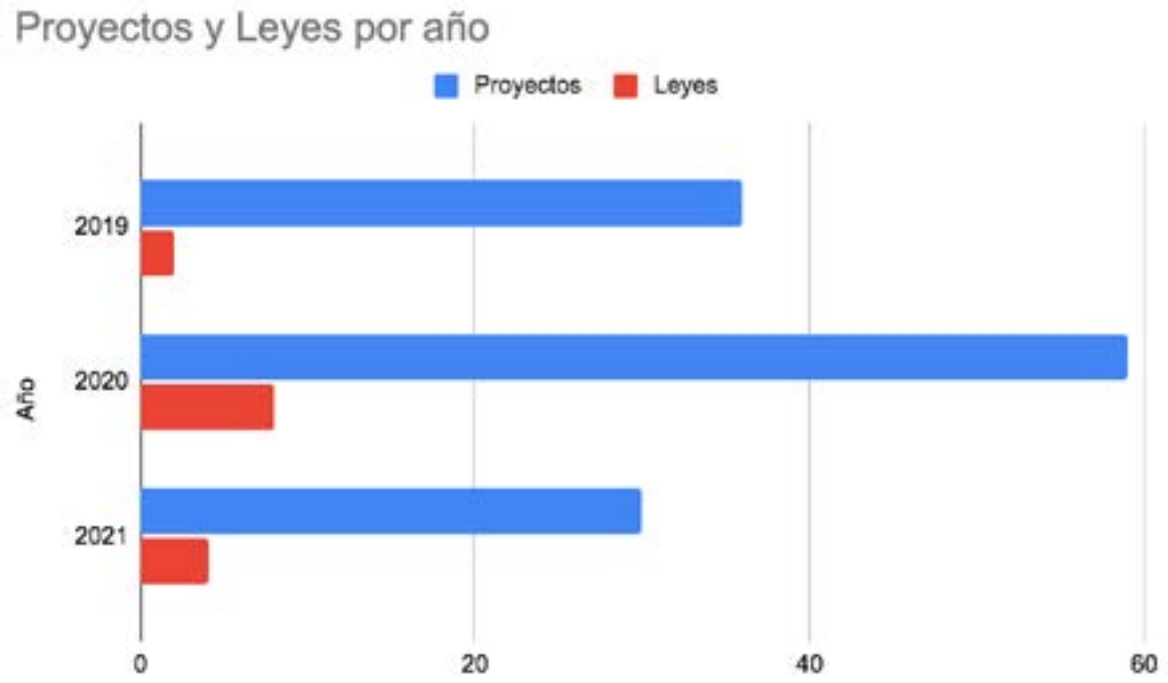
2.1. Balance general

Desde el 1° de enero de 2019 y hasta el 30 de septiembre de 2021, se tramitó –en los nueve países objeto de revisión– un total de 125 proyectos de ley (90,4%) y 14 leyes (9,6%) en protección de datos.[89] En 2019, se tramitó un total de 36 proyectos de ley y 2 leyes; en 2020, se dio curso a 59 proyectos de ley y 8 leyes; y, en lo que va corrido del 2021, se ha dado curso a un total de 30 proyectos de ley y 4 leyes. El año 2020 fue el de mayor actividad legislativa en la región en materia de protección de datos.

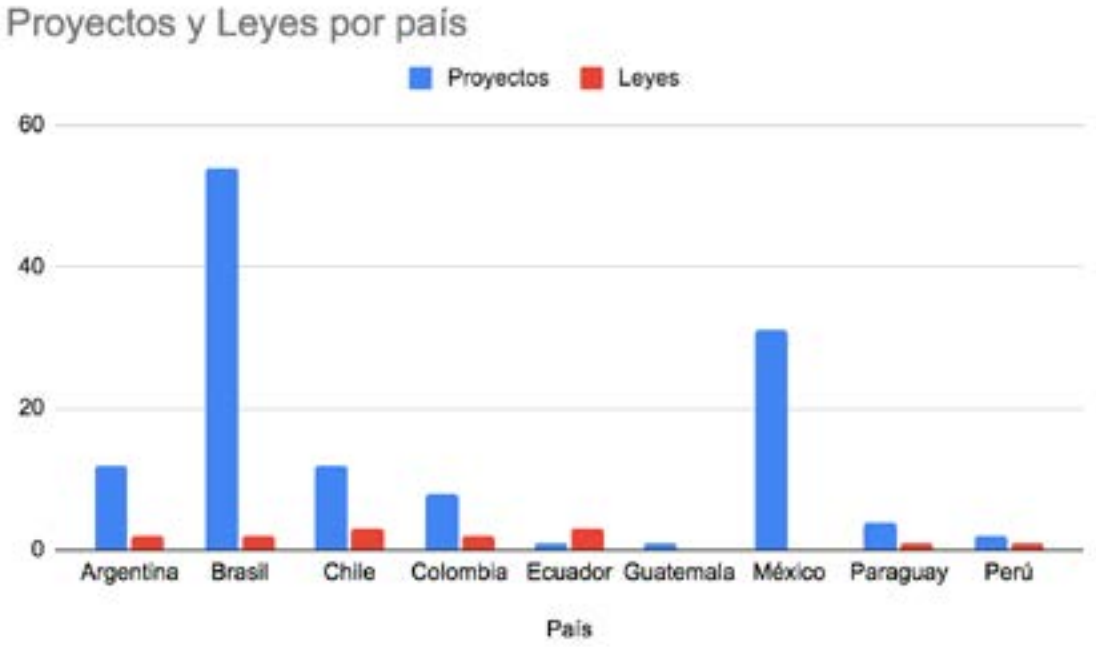
87 En este sentido, sugerimos leer los comentarios que organizaciones de la sociedad civil enviaron a la Red Iberoamericana de Protección de Datos a propósito del borrador de declaración sobre "Violencia digital en mujeres y niñas". Ver, Fundación Karisma, "Comentarios al borrador de declaración sobre 'Violencia digital en mujeres y niñas'", 2021, disponible en: https://web.karisma.org.co/comentarios-al-borrador-de-declaracion-sobre-violencia-digital-en-mujeres-y-ninas, último acceso: 13 de abril de 2022.

88 En su informe, Cannataci apunta que los reclusos también tienen derecho a la privacidad que se orientan bajo reglas especiales. Ver, ONU, Asamblea General, *supra* nota 86, § 32.

89 De acuerdo con lo advertido en la introducción, se incluyeron proyectos de ley que refieren en su título al derecho a la protección de datos y otros que por su contenido integran previsiones que impactan en el ejercicio de este derecho. Se integraron proyectos de ley y leyes que referían al impacto en el derecho a la protección de datos en línea y fuera de ella.



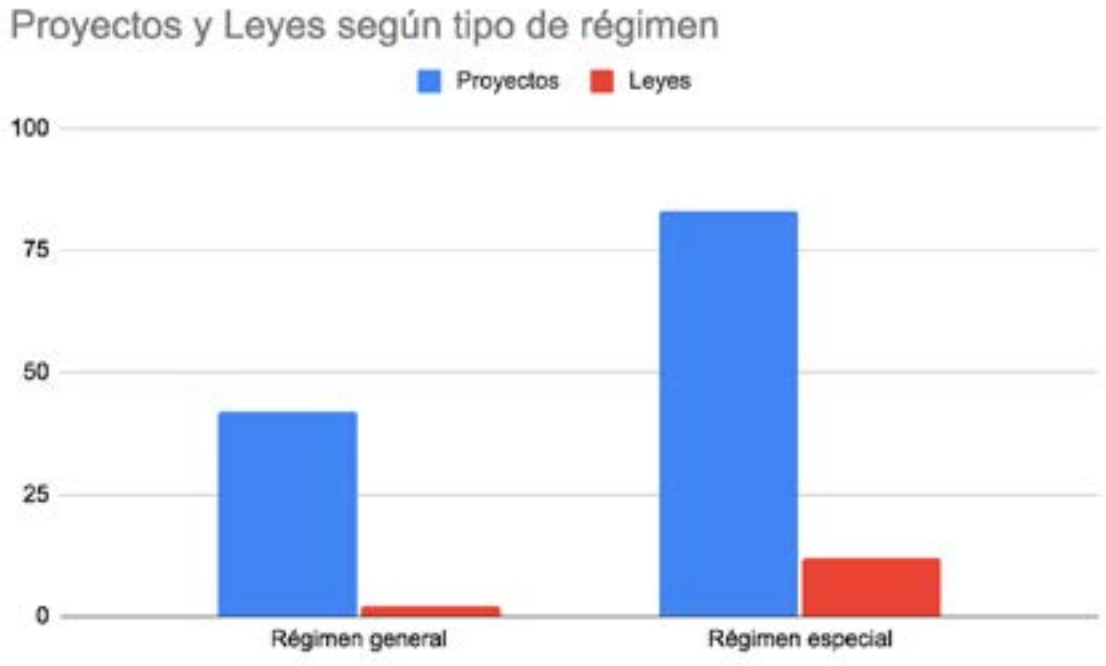
En su origen por país, los datos son los siguientes: Argentina (12 proyectos de ley, 2 leyes); Brasil (54 proyectos de ley, 2 leyes); Chile (12 proyectos de ley, 3 leyes); Colombia (8 proyectos de ley, 2 leyes); Ecuador (1 proyecto de ley, 3 leyes); Guatemala (1 proyecto de ley, 0 leyes); México (31 proyectos de ley, 0 leyes); Paraguay (4 proyectos de ley, 1 ley); y Perú (2 proyectos de ley, 1 ley). El país más activo en la materia es Brasil, seguido de México y Argentina.



Según la autoridad de origen, la presentación de proyectos de ley en protección de datos fue así: Senado (42 proyectos, 7 leyes); Cámara (84 proyectos, 3 leyes); Cámara Única (6 proyectos, 4 leyes).

Los proyectos de ley que tienen origen en la Cámara de Diputados o Representantes de los países son más numerosos, sin embargo, la brecha entre los que se tramitan y terminan convertidos en ley es alta. Pese a que los Congresos con Cámara Única tienen una actividad legislativa reducida en materia de protección de datos, la distancia que separa el número de proyectos en trámite y las leyes sancionadas es menor.

Ahora, en relación a la protección de datos, distinguimos entre dos regímenes. El "régimen general" en el que incluyeron los proyectos de ley y leyes que regulan su ejercicio de manera transversal para el sector público y privado, y que aplican sin distinción del sector económico, tipo de actividad, responsable o tipo de dato objeto del tratamiento; así como los proyectos de ley y leyes modificatorios de los regímenes generales de protección de datos. En el "régimen especial", se incluyeron los proyectos de ley y leyes que regulan su ejercicio según un tipo específico de actividad, responsable, dato personal, titular del dato o tecnología digital.



Los resultados, en este sentido, fueron los siguientes: en el régimen general (41 proyectos de ley, 2 leyes); y en el régimen especial (91 proyectos de ley, 12 leyes). En los países analizados, la actividad legislativa sigue atendiendo asuntos con-

cretos o especiales. Allí predominan los proyectos de ley según tipos de sector, actividad, titular del dato, entre otros, tal y como veremos a continuación.

Por último, sobre los temas de la actividad legislativa en protección de datos en los nueve países, se hizo una agrupación para facilitar el análisis. La propuesta de grupos –que reúnen en algunos casos a otros subgrupos de temas– es la que sigue:

1. Grupo de iniciativas sobre generalidades en el tratamiento la protección de datos

Incluye a su vez ocho subgrupos que comprenden al ejercicio general de derechos ARCO[90] –y otros derechos y principios–; a la existencia o a las facultades de la autoridad de protección de datos personales; a la creación de regímenes generales de tratamiento de datos; a los aspectos de seguridad en el tratamiento; a los mecanismos de autorregulación o buenas prácticas; a la creación del "derecho al olvido"; a los aspectos de aplicabilidad o alcance legal del régimen de protección de datos.

Entre dicho grupo, los temas con la mayor actividad legislativa en el trámite de proyectos de ley y leyes en su orden fueron: la regulación sobre el ejercicio de los derechos ARCO –y otros derechos u principios– (7 proyectos de ley, 0 leyes); la regulación del tratamiento general de datos personales (3 proyectos de ley, 1 ley); la regulación del "derecho al olvido" (5 proyectos de ley, 0 leyes); la regulación sobre aspectos de seguridad digital en el tratamiento de datos (4 proyectos de ley, 0 leyes); la regulación sobre mecanismos de autorregulación y buenas prácticas (2 proyectos, 0 leyes); la regulación sobre el alcance o la aplicación del régimen de protección de datos (1 proyecto de ley, 1 ley); la regulación sobre excepciones en la aplicación de las leyes de protección de datos (1 proyecto de ley, 0 leyes); la regulación sobre la autoridad de protección de datos (1 proyecto de ley, 1 ley).

2. Grupo de iniciativas sobre el tratamiento de datos por sector, actividad y responsable

Incluye nueve subgrupos sobre la regulación del tratamiento en el sector financiero, educativo, de la salud, laboral y de las telecomunicaciones; en las actividades de publicidad; en las actividades electorales; en las actividades de identificación de la ciudadanía; y en el tratamiento efectuado por entidades públicas.

Los temas de mayor actividad legislativa en el trámite de proyectos y leyes en su

[90] En este tema, se encuentran reunidas las iniciativas que reconocen el derecho a la portabilidad de datos, a la interoperabilidad y a la indemnización a la persona por afectaciones sufridas en el tratamiento de sus datos.

orden fueron: tratamiento de datos en el sector financiero (12 proyectos, 0 leyes); tratamiento en el sector de la salud (6 proyectos, 2 leyes); en las actividades de identificación de la ciudadanía (3 proyectos, 2 leyes); en las actividades electorales (3 proyectos, 2 leyes); tratamiento en el sector educativo (3 proyectos, 0 leyes); tratamiento en las actividades de publicidad (3 proyectos, 0 leyes); tratamiento en el sector de las telecomunicaciones (2 proyectos, 0 leyes); tratamiento en el ámbito laboral (1 proyecto, 1 ley).

3. Grupo de iniciativas sobre el tratamiento según tipos de titulares y tipos de datos

Incluye seis subgrupos sobre el ejercicio de la protección de datos de niños, niñas y adolescentes (4 proyectos de ley, 0 leyes); de adultos mayores (1 proyecto de ley, 0 leyes); de consumidores (2 proyectos de ley, 0 leyes); el ejercicio post mórtem[91] (6 proyectos de ley, 0 leyes); y la regulación de los datos sensibles[92] (15 proyectos de ley, 2 leyes).

Los temas de mayor actividad legislativa en el trámite de proyectos de ley y leyes en su orden fueron: la regulación de los datos sensibles (15 proyectos de ley, 2 leyes); el ejercicio del derecho a la protección de datos post mórtem (6 proyectos de ley, 0 leyes); el ejercicio de la protección de datos de niños, niñas y adolescentes (4 proyectos de ley, 0 leyes); de consumidores (2 proyectos de ley, 0 leyes); y de adultos mayores (1 proyecto de ley, 0 leyes).

4. Grupo de iniciativas sobre el tratamiento de datos ejercido en internet y a través de otras tecnologías digitales

En este grupo, se han tramitado 23 proyectos de ley y ninguna ley. Se incluyeron las iniciativas que regulan el ejercicio del derecho a la protección de datos en internet y a través del uso de otras tecnologías digitales.[93]

5. Grupo de iniciativas sobre el tratamiento de datos con ocasión de la pandemia

En este grupo se han tramitado 10 proyectos de ley y ninguna ley. Se clasificó como iniciativa de pandemia a todas las que refieren a la extensión de plazos en los re-

[91] En este se incluyeron iniciativas sobre el tratamiento de datos de personas fallecidas, testamento digital, destino de los datos de personas fallecidas y uso de imágenes de personas fallecidas.

[92] En este se incluyeron iniciativas sobre el uso de datos biométricos y datos genéticos.

[93] En este se incluyeron iniciativas sobre la protección de datos en el uso de criptomonedas y blockchain; en redes sociales; en plataformas de domicilios; en el uso de vants y drones; y en el uso de sistemas de inteligencia artificial y automatización de decisiones.

portes de mora en el pago de obligaciones crediticias o financieras producto de la crisis económica ocasionada por el covid-19; a la extensión de plazos en las sanciones relacionadas a la ley de protección de datos debido a la emergencia sanitaria; al tratamiento de datos para la selección de beneficiarios de ayudas económicas; al tratamiento de datos en el ámbito sanitario mientras tenga vigencia la pandemia.

6. Grupo de iniciativas "otros"

En este grupo (5 proyectos de ley, 1 ley), se encuentran iniciativas únicas y que no pertenecen a ninguno de los grupos anteriores. Los temas a los que refieren van desde la protección de datos en la prevención de hechos de corrupción; al tratamiento de datos en la recolección de la evidencia digital; hasta el deber de incluir el desarrollo del derecho a la protección de datos en políticas públicas que las iniciativas legales ordenan desarrollar.

VI. Análisis por países

En el siguiente análisis, acudimos a los criterios de caracterización del contenido de las iniciativas en privacidad y protección de datos que han tenido curso en Argentina, Brasil, Chile, Colombia, Ecuador, Guatemala, México, Paraguay y Perú. Recomendamos ir a la sección de anexos pues esta informa sobre la regulación a nivel constitucional de cada materia; la existencia o no de una ley; la autoridad y el mecanismo para la defensa del derecho a la protección de datos; la regulación de base de vigilancia de las comunicaciones; las autoridades facultadas para llevar a cabo actividades de dicho tipo y el tipo de orden que las faculta para su ejecución.

1. Argentina

1.1 Privacidad: 1 proyecto de ley, 2 leyes

Las dos leyes aprobadas son el Código Procesal Penal Federal y el Programa Nacional de Prevención contra el Ciberacoso y el Grooming contra Niños, Niñas y Adolescentes. El proyecto de ley en curso trata la modificación del Código Penal argentino para prever la difusión no consentida de imágenes con contenido íntimo o sexual.

El balance general en materia de privacidad es el siguiente:

- *Medidas que introducen.* El Código Procesal Penal introduce nuevas disposi-

ciones sobre las actividades de vigilancia de las comunicaciones. El proyecto de código penal prevé las medidas de investigación de abusos a la privacidad de las personas y dispone medidas de otro tipo, como de sensibilización, de concientización, etc.

- *Orden que limita o restringe el ejercicio del derecho a la privacidad.* En el Código Procesal Penal se prevé que la orden que limita la privacidad de las comunicaciones sea judicial y previa. La reforma al Código Penal dispone la orden judicial posterior –sentencia– y en el Programa Nacional contra el Grooming y Ciberacoso no se especifica el dictado de medidas de limitación o restricción a derechos.
- *Actividades que regula.* El Código Procesal Penal Federal se refiere a las actividades de interceptación de las comunicaciones, así como a los procesos de "secuestro" o "incautación" de los datos, que puede entenderse como un procedimiento similar al acceso directo, en tanto que no intermedia ni puede oponerse a su ejecución ningún tercero. El proyecto de ley y la otra ley no determinan nada en este sentido.
- *Estándares de la orden que limita el derecho a la privacidad.*
- *Deberes y derechos que reconoce.* Solo la política nacional contra el grooming y el ciberacoso consagra el deber de prevención a cargo de las entidades públicas obligadas.
- *Tecnologías digitales.* Solo la política nacional contra el grooming y el ciberacoso prevé que las actividades de prevención deben orientarse al uso de redes sociales y dispositivos tecnológicos.

1.2 Protección de datos: 12 proyectos de ley, 2 leyes

La actividad legislativa del país ha abordado temas diversos. Desde la prescripción electrónica; el Programa de Inclusión Digital para Adultos Mayores; las iniciativas que regulan el "derecho al olvido", el envío de publicidad no deseada y el tratamiento de datos en el trabajo; un proyecto de ley para crear una nueva ley de protección de datos personales; y proyectos de ley que redefinen el concepto de la Ley de Protección de Datos Personales vigente, en lo que tiene que ver con la inclusión de los datos sensibles.

El balance general de la caracterización de su contenido es el siguiente:

- *Mecanismos de protección.* La mayoría reconoce la existencia de mecanismos de protección de tipo judicial, administrativo o mixto (5 proyectos de ley, 1 ley).
- *Derechos que reconoce.* La mayoría de proyectos, salvo las leyes, reconoce al titular del dato el ejercicio de los derechos ARCO o remite a lo consagrado en materia de derechos en la Ley de Protección de Datos Personales existente.
- D*atos sensibles.* Solo 2 proyectos de ley autorizan el tratamiento de datos sensibles como regla general. Uno afirma su prohibición a través de la vía penal en la que integra la pena de cárcel por la difusión o el tratamiento no consentido, y el otro proyecto de ley (de tratamiento de datos personales) prohíbe su tratamiento con la indicación de excepciones.
- *Tecnologías digitales.* Las iniciativas sobre el tratamiento de datos con fines publicitarios prevén el uso de tecnologías para la recolección y el perfilamiento comercial, y un par de proyectos de ley prevén el uso de tecnologías de autenticación o identificación biométrica.
- *Flujo transfronterizo de datos.* Solo el proyecto de ley que crea una nueva ley de protección de datos personales reconoce como estándar el nivel adecuado de protección para el flujo de datos personales a terceros países.
- *Excepciones en su aplicación.* Solo el proyecto de ley de protección de datos personales dispone como excepciones en su aplicación al tratamiento de uso personal o que ocurre en el ámbito familiar, así como excepciones al ejercicio de los derechos ARCO cuando se lleva a cabo el tratamiento en actividades de seguridad, en el cuidado de la salud, en la investigación de delitos penales, entre otros.
- *Privacidad por diseño y por defecto.* Solo el proyecto de ley de protección de datos personales prevé a cargo de los responsables del tratamiento de datos la adopción de medidas de protección de la privacidad desde el diseño y por defecto.
- *Autoridad de protección.* La mayoría de las iniciativas delega a la autoridad de protección de datos y a otras autoridades facultades sobre su contenido en materia de protección de datos.
- *Facultades de la autoridad.* La mayoría de las iniciativas no advierte nada en este sentido, salvo el proyecto de ley que crea una ley general de protección de datos.

2. Brasil

2.1 Privacidad: 11 proyectos de ley, 1 ley

En buena medida, los proyectos de ley relevados apuntan a modificar la ley N° 9.296 de 1996 sobre interceptación de las comunicaciones para añadir nuevas actividades a las ya previstas en ese marco legal. La ley sancionada es el Código Penal y de Procedimiento Penal que también integra modificaciones en dicho tema. Se destaca el proyecto de ley que prevé como delito la difusión en fuentes abiertas de los datos personales de los agentes de policía, y otro más castiga la recolección y la difusión de datos personales de manera indebida, obtenidos a propósito de la realización de actividades de interceptación de las comunicaciones.

El balance general en materia de privacidad es el siguiente:

- *Medidas que introducen.* La mayoría de las iniciativas regula las actividades de vigilancia individualizada de las comunicaciones. 1 proyecto de ley se refiere a las actividades de vigilancia masiva, y un par de proyectos de ley reglamentan los abusos a la privacidad de las personas.
- *Orden que limita o restringe el ejercicio del derecho a la privacidad.* La mayoría de los proyectos de ley que modifica el contenido de la ley N° 9.296 remite a su contenido, y otros reiteran la necesidad de una orden judicial previa.
- *Actividades que regula.* La ley sancionada se refiere a la interceptación de las comunicaciones; otros proyectos de ley regulan actividades como el acceso directo, el monitoreo del espectro electromagnético y la solicitud de datos de los suscriptores de las compañías de telecomunicaciones.
- *Estándares de la orden que limita el derecho a la privacidad.* Solo 1 proyecto de ley indica que la orden judicial previa, que autoriza la interceptación de las comunicaciones, debe satisfacer el estándar de la motivación fundada, so pena de nulidad. El resto no advierte nada en este sentido.
- *Deberes y derechos que reconoce.* La mayoría de los proyectos de ley no advierte nada sobre el particular.
- *Tecnologías digitales.* Algunos proyectos de ley hacen alusión a las tecnologías de interceptación e internet.

2.2 Protección de datos: 54 proyectos de ley, 2 leyes

Una cantidad considerable de proyectos de ley se dirigen a modificar la reciente Ley General de Protección de Datos y el Marco Civil de Internet para introducir previsiones sobre protección de datos en internet. Varias iniciativas se encuentran dirigidas a regular el uso de biometría para fines diversos, como la autenticación de estudiantes en el sector educativo y de las personas en el pago de transacciones, entre otros. Otras iniciativas también se dirigen a regularizar el destino de los datos de las personas fallecidas –o tratamiento post mórtem–, a regular el tratamiento de datos en actividades de telemedicina; a crear el registro de datos personales de personas condenadas; entre otros.

El balance general de la caracterización de su contenido es el siguiente:

- *Mecanismos de protección.* Solo una minoría de las iniciativas legales advierte sobre la existencia de mecanismos de protección de tipo judicial y administrativo (12 proyectos de ley, 1 ley).
- *Derechos que reconoce.* Solo 8 proyectos de ley y 1 ley remiten a lo consagrado en la Ley General de Protección de Datos, y apenas algunos reconocen por su cuenta un conjunto de principios para orientar el tratamiento de datos.
- *Datos sensibles.* 17 proyectos de ley y 1 ley autorizan como regla general el tratamiento de datos sensibles; solo 2 proyectos de ley prohíben su tratamiento como regla general.
- *Tecnologías digitales.* Al menos 13 proyectos de ley contemplan previsiones sobre el tratamiento de datos en internet; 5 proyectos de ley determinan el procesamiento automatizado o semiautomatizado de datos; 8 proyectos de ley hacen referencia al uso de sistemas de identificación o de verificación biométrica; y 1 proyecto de ley establece el uso de tecnologías para el perfilamiento comercial.
- *Flujo transfronterizo de datos.* Ningún proyecto de ley consagró previsiones en este sentido.
- *Excepciones en su aplicación.* Solo 1 proyecto de ley incluye excepciones en la aplicación de la normativa sobre la protección de datos a favor de la libertad de prensa.
- *Privacidad por diseño y por defecto.* Solo 2 proyectos de ley refieren al deber que tienen los responsables de datos de integrar medidas de protección a la privacidad y a la seguridad desde el diseño y por defecto.

- *Autoridad de protección.* Solo 6 proyectos de ley delegan competencia sobre su contenido a la autoridad de protección de datos creada por la Ley General de Protección de Datos.
- *Facultades de la autoridad.* La mayoría de los proyectos de ley no provee información en este sentido.

3. Chile

3.1 Privacidad: sin actividad legislativa en la materia
Protección de datos: 12 proyectos de ley, 3 leyes

En este país, la gran mayoría de los proyectos de ley está destinada a la regulación del tratamiento de datos en el sector crediticio o financiero, algunos de ellos asociados a la emergencia sanitaria. El conjunto de leyes sancionadas es diverso: una reglamenta la transformación digital del Estado (y contiene previsiones sobre el tratamiento de datos sensibles), otra regula la protección de datos en materia financiera o crediticia, y la última ordena desarrollar una política pública de lucha contra el cáncer que prevea disposiciones en materia de protección de datos.[94]

El balance general de la caracterización de su contenido es el siguiente:

- *Mecanismos de protección.* La totalidad de las iniciativas no especifica qué mecanismos tiene la persona para ejercer el control de su información personal.
- *Derechos que reconoce.* La mayoría de los proyectos de ley no precisa qué derechos se reconocen al titular del dato (10 proyectos de ley), salvo el derecho a la mora en el reporte de obligaciones atrasadas o impagas, que no constituye un derecho en materia de protección de datos, sino un beneficio legal en consideración del contexto económico actual. Lo mismo sucede con el beneficio de prohibición de comunicación de los reportes negativos por razones similares.
- *Datos sensibles.* Solo 1 ley se refiere a la autorización para su tratamiento como regla general.
- *Tecnologías digitales.* La totalidad de los proyectos de ley no advierte qué tipo de tecnologías digitales son usadas o desplegadas para el tratamiento de datos.

[94] Las previsiones de datos personales se refieren a propósito de la necesidad de mantener la confidencialidad de los datos de las personas, restringir su acceso a terceros no autorizados, y afirman el uso de datos personales en salud solo para los fines que sean advertidos por el Plan Nacional del Cáncer.

- *Flujo transfronterizo de datos.* La totalidad no prevé nada en este sentido.
- *Excepciones en su aplicación.* Ningún proyecto de ley dispone excepciones en su aplicación.
- *Privacidad por diseño y por defecto.* Ningún proyecto de ley prevé ajustes en este sentido.
- *Autoridad de protección.* Ningún proyecto de ley indica una autoridad competente sobre su contenido en materia de protección de datos.
- *Facultades de la autoridad.* No prevén el ejercicio de facultades a cargo de autoridad de protección de datos alguna.

4. Colombia

4.1 Privacidad: 2 proyectos de ley, 0 leyes

Se trata de dos proyectos de ley que fueron archivados, uno que pretendía regular la difusión no consentida de imágenes con contenido sexual, y otro que modificaba el marco legal de inteligencia para incluir las actividades de monitoreo del espectro electromagnético, así como la modificación de la previsión legal sobre el deber que tienen las empresas de telecomunicaciones de entregar los datos de sus suscriptores, con una orden judicial previa en el marco de una investigación penal.

El balance general en materia de privacidad es el siguiente:

- *Medidas que introducen.* Una iniciativa aborda las facultades de las actividades de vigilancia de las comunicaciones, la otra regulariza el ejercicio de la privacidad junto a otros derechos.
- *Orden que limita o restringe el ejercicio del derecho a la privacidad.* El proyecto de ley, que buscaba modificar la Ley de Inteligencia y Contrainteligencia, no especifica qué tipo de orden puede autorizar las actividades de monitoreo del espectro, sin embargo, sí prevé la existencia de una orden judicial previa para ordenar a las empresas de telecomunicaciones la entrega de los datos de sus suscriptores.
- *Actividades que regula.* 1 proyecto de ley regula el monitoreo del espectro, y advierte que se dirige a una vigilancia generalizada, la cual no debe impactar en el ejercicio de los derechos humanos, y el otro proyecto de ley reglamenta la investigación penal del delito de difusión no consentida.

- *Estándares de la orden que limita el derecho a la privacidad.* No proveen información en este sentido.
- *Deberes y derechos que reconoce.* El proyecto de ley que modificaba la Ley de Inteligencia y Contrainteligencia reconoce el deber de supervisión, pero reserva el contenido de los informes de rendición de cuentas.
- *Tecnologías digitales.* Solo el proyecto de ley de difusión no consentida se refiere a la difusión que tiene lugar en internet.

4.2 Protección de datos: 8 proyectos de ley, 2 leyes

En esta materia, se ha dado curso a las iniciativas de tipo disímil: desde el ejercicio del habeas data en el sector financiero; pasando por la creación del Banco Nacional de Datos Genéticos; la regulación de la protección de datos en el nuevo Código Electoral; la historia clínica electrónica; el tratamiento de datos para la identificación de conductores; hasta la sanción reciente de su política migratoria que autoriza el uso de biometría en la identificación de migrantes.

El balance general de la caracterización de su contenido es el siguiente:

- *Mecanismos de protección.* La mayoría de los proyectos de ley y las leyes no especifica qué mecanismos tiene la persona para ejercer el control de su información personal (5 proyectos de ley, 2 leyes).
- *Derechos que reconoce.* La mayoría de los proyectos de ley no precisa qué derechos se reconocen al titular del dato (3 proyectos de ley).
- *Datos sensibles.* La mayoría de los proyectos de ley no especifica reglas en torno a su tratamiento (4 proyectos de ley).
- *Tecnologías digitales.* La mayoría de los proyectos de ley no refiere al tipo de tecnologías digitales que serán empleadas para la recolección o el procesamiento de los datos (6 proyectos de ley).
- *Flujo transfronterizo de datos.* Ningún proyecto de ley prevé estándar alguno sobre la recolección o el flujo transfronterizo de datos a terceros países.
- *Excepciones en su aplicación.* Ningún proyecto de ley contempla excepciones favorables a la libertad de prensa, la seguridad nacional o las emergencias sanitarias en su aplicación.

- *Privacidad por diseño y por defecto.* Ningún proyecto de ley prevé ajustes en este sentido.
- *Autoridad de protección.* De forma mayoritaria, las iniciativas delegan competencia sobre su contenido a distintas autoridades de protección de datos (3 proyectos de ley, 1 ley).
- *Facultades de la autoridad.* Mayoritariamente, las iniciativas no detallan qué facultades tiene esa otra autoridad sobre el contenido de los proyectos de ley y ley en materia de protección de datos (3 proyectos de ley, 1 ley).

5. Ecuador

5.1 Privacidad: sin actividad legislativa en la materia
Protección de datos: 1 proyecto de ley, 3 leyes

Entre las leyes sancionadas recientemente, se encuentran el Régimen General de Protección de Datos, el Código Electoral y la Ley Orgánica de Actuación en Casos de Personas Extraviadas y Desaparecidas, así como un proyecto de ley sobre la gestión de la identidad de las personas, que refiere al tratamiento de datos personales.

El balance general de la caracterización de su contenido es el siguiente:

- *Mecanismos de protección.* Solo la Ley Orgánica de Protección de Datos Personales prevé mecanismos de protección de tipo administrativo.
- *Derechos que reconoce.* Solo la Ley Orgánica de Protección de Datos Personales reconoce el ejercicio de los derechos ARCO a favor del titular.
- *Datos sensibles.* Solo la Ley Orgánica de Protección de Datos Personales prohíbe su tratamiento como regla general y la Ley Orgánica de Actuación en Casos de Personas Extraviadas y Desaparecidas autoriza su tratamiento por regla general.
- *Tecnologías digitales.* Solo la Ley Orgánica de Protección de Datos Personales refiere al tratamiento a través de tecnologías digitales de toma de decisiones automatizadas o semiautomatizadas.
- *Flujo transfronterizo de datos.* La Ley Orgánica de Protección de Datos Personales integra el nivel adecuado de protección como estándar para permitir el flujo de datos a terceros países.

- *Excepciones en su aplicación.* Solo la Ley Orgánica de Protección de Datos Personales incorpora excepciones en su aplicación en eventos de emergencias sanitarias.
- *Privacidad por diseño y por defecto.* Únicamente la Ley Orgánica de Protección de Datos Personales incluye esta previsión.
- *Autoridad de protección.* La Ley Orgánica de Protección de Datos Personales crea una autoridad de protección de datos sobre la cual delega la competencia de su contenido, y la Ley Orgánica de Actuación en Casos de Personas Extraviadas y Desaparecidas delega la competencia en dicha materia a otra autoridad.
- *Facultades de la autoridad.* En su mayoría, no especifican las facultades de la autoridad competente, salvo la Ley Orgánica de Protección de Datos Personales que refiere a las facultades de investigación, vigilancia y control.

6. Guatemala

6.1 Privacidad: sin actividad legislativa en la materia
Protección de datos: 1 proyecto de ley, 0 leyes

El proyecto de ley en trámite crea un banco de datos genéticos con fines de identificación forense. El balance general de la caracterización de su contenido es el siguiente:

- *Mecanismos de protección.* No especifica qué mecanismos tiene la persona para ejercer el control de su información personal.
- *Derechos que reconoce.* No especifica qué derechos tiene el titular del dato. En todo caso, prevé la eliminación de la información a los 80 días siguientes de ser registrada.
- *Datos sensibles.* Autoriza por regla general su tratamiento.
- *Tecnologías digitales.* No determina nada en este sentido.
- *Flujo transfronterizo de datos.* Dispone como estándar la reciprocidad y la confidencialidad de la información, bajo estándares de seguridad y privacidad sin proveer más detalles al respecto.
- *Excepciones en su aplicación.* No especifica nada en este sentido.
- *Privacidad por diseño y por defecto.* No detalla nada en este sentido.

- *Autoridad de protección.* Delega la competencia sobre su contenido a otras autoridades al considerar, entre otras cosas, que no tiene autoridad de protección de datos.
- *Facultades.* No refiere a nada en este sentido, salvo la facultad de conformación de la base de datos.

7. México

7.1 Privacidad: 7 proyectos de ley, 1 ley

Los proyectos de ley apuntan a la modificación del Código Penal Federal para cambiar la facultad de interceptación de las comunicaciones y castigar los delitos de difusión de datos personales de menores de edad; a la creación de bases de datos de agresores sexuales; y a modificar la Ley Federal de Telecomunicaciones. La ley sancionada es la Ley Olimpia sobre difusión no consentida de imágenes con contenido sexual.

El balance general en materia de privacidad es el siguiente:

- *Medidas que introducen.* La mayoría de las iniciativas regula la vigilancia individualizada de las comunicaciones vinculada a investigaciones judiciales.
- *Orden que limita o restringe el ejercicio del derecho a la privacidad.* En los proyectos de ley que modifican las facultades de interceptación, se reconoce la necesidad de una orden judicial previa, y solo en una iniciativa se habilita la interceptación de las comunicaciones mediante orden administrativa de cuerpos de policía, entre otros.
- *Actividades que regula.* Entre las actividades que se regulan, se encuentran la interceptación de las comunicaciones, la solicitud de datos de los suscriptores de los servicios de telecomunicaciones y la investigación penal de los abusos a la privacidad.
- *Estándares de la orden que limita el derecho a la privacidad.* No se provee información en este sentido.
- *Deberes y derechos que reconoce.* Solo hay 1 proyecto de ley que reconoce el deber de rendición de cuentas sobre las actividades de interceptación, que tendrá lugar ante el Poder Legislativo.

- *Tecnologías digitales.* Solo en un par de proyectos de ley se hace referencia expresa a internet.

7.2 Protección de datos: 31 proyectos de ley, 0 leyes

La mayoría de las iniciativas apunta a modificar el Régimen General o Federal de Protección de Datos para cambiar definiciones, reconocer otros derechos como el "derecho al olvido" y regular su ejercicio en internet o plataformas digitales. Algunos se dirigen a reglamentar el tratamiento de datos post mórtem, así como proyectos sobre la protección de datos en el sector financiero y educativo. También se encuentran en trámite un proyecto de ley que crea la ley de identificación personal, y varios otros que reconocen y regulan la titularidad del derecho al tratamiento de datos de niños, niñas y adolescentes.

El balance general de la caracterización del contenido de las iniciativas es el siguiente:

- *Mecanismos de protección.* Solo 7 proyectos de ley refieren a la existencia de mecanismos de protección de tipo administrativo y judicial.
- *Derechos que reconoce.* La mayoría de las iniciativas reconoce otros derechos distintos a los derechos ARCO, como el "derecho al olvido", el derecho a obtener una indemnización por el indebido tratamiento de los datos, el derecho a la seguridad, el de no ser contactado para fines publicitarios, a la notificación frente a brechas y vulnerabilidades de seguridad, el derecho a que la persona determine el destino de sus datos y este se cumpla después de su muerte, y el derecho a la portabilidad.
- *Datos sensibles.* Solo 4 proyectos de ley refieren a la autorización como regla general para el tratamiento de los datos sensibles.
- *Tecnologías digitales.* Al menos 6 proyectos de ley se refieren al tratamiento de datos a través de internet. 2 proyectos de ley se refieren al uso de tecnologías de verificación y autenticación biométrica.
- *Flujo transfronterizo de datos.* Solo el proyecto de ley que crea la ley de identificación personal prevé como estándar el nivel adecuado de protección para facilitar el intercambio de datos a terceros países.
- *Excepciones en su aplicación.* 1 proyecto de ley consagra excepciones en su aplicación en materia de seguridad nacional, y otro está más a favor de la libertad de prensa.

- *Privacidad por diseño y por defecto.* Ningún proyecto de ley tiene previsiones en este sentido.
- *Autoridad de protección.* Al menos 6 proyectos de ley delegan competencia sobre su contenido a la autoridad de protección de datos, y algunos delegan competencia a otras autoridades.
- *Facultades de la autoridad.* Solo 3 proyectos de ley prevén como facultades de la autoridad encargada vigilar, investigar y sancionar.

8. Paraguay

8.1 Privacidad: sin actividad legislativa en la materia
Protección de datos: 4 proyectos de ley, 1 ley

El país se encuentra en el trámite de diversas iniciativas para introducir un régimen general de protección de datos, así como en la regulación del uso de biometría para los sistemas de identificación en el servicio de telefonía móvil y para fines electorales. Sancionó, recientemente, una reforma a la Ley de Datos Personales Crediticios.

El balance general de la caracterización del contenido de las iniciativas es el siguiente:

- *Mecanismos de protección.* Las iniciativas refieren a mecanismos de protección de tipo administrativo (1 proyecto de ley, 1 ley) y, al tiempo, de tipo administrativo y judicial (1 proyecto de ley).
- *Derechos que reconoce.* De forma mayoritaria, se reconoce el conjunto de derechos ARCO a su titular (2 proyectos de ley, 1 ley).
- *Datos sensibles.* En 2 proyectos de ley y 1 ley, se prohíbe su tratamiento por regla general.
- *Tecnologías digitales.* En 2 proyectos de ley, se hace referencia al uso de sistemas de biometría y en 1 proyecto de ley al procesamiento automatizado o semiautomatizado de datos personales.
- *Flujo transfronterizo de datos.* Solo 1 proyecto de ley prevé la adopción del nivel adecuado de protección para llevar a cabo el intercambio de datos a terceros países.
- *Excepciones en su aplicación.* En 2 proyectos de ley, se contemplan excepciones a favor de la seguridad nacional.

- *Privacidad por diseño y por defecto.* En su mayoría, no especifican.
- *Autoridad de protección.* Delega la competencia sobre su contenido a otras autoridades al considerar, entre otras cosas, que no tiene autoridad de protección de datos.
- *Facultades de la autoridad.* En 2 proyectos de ley y 1 ley, se prevén las facultades de investigación, vigilancia y sanción.

9. Perú

9.1 Privacidad: 3 proyectos de ley, 1 ley

Se trata de proyectos de ley que regulan en dos versiones distintas las actividades de ciberseguridad, otro proyecto sobre el acceso a los sistemas de videovigilancia públicos y privados para la lucha en materia de seguridad ciudadana, y la más recientemente sancionada ley que faculta a la policía nacional a acceder a los datos de las comunicaciones de las personas para combatir el crimen organizado.

El balance general en materia de privacidad es el siguiente:

- *Medidas que introducen.* En su mayoría, los proyectos de ley refieren a las actividades o a las autoridades facultadas para llevar a cabo actividades de vigilancia de las comunicaciones.
- *Orden que limita o restringe el ejercicio del derecho a la privacidad.* En 1 proyecto de ley y la ley vigente, la orden para llevar a cabo estas actividades es de tipo administrativo. En el caso particular de la ley, la orden es emitida por la policía nacional y no se prevé o advierte nada sobre su control judicial posterior.
- *Actividades que regula.* La ley vigente dispone tanto el acceso directo como la solicitud de datos de los usuarios de los servicios de telecomunicaciones, y uno de los proyectos de ley de ciberseguridad prevé el ciberpatrullaje electoral.
- *Estándares de la orden que limita el derecho a la privacidad.* Ninguna de las iniciativas en trámite, incluida la que fue sancionada, establece la atención de los estándares interamericanos.
- *Deberes y derechos que reconoce.* La mayoría no reconoce derechos ni deberes de los que se advierten en cabeza de los Estados por el sistema interamericano.
- *Tecnologías digitales.* La mayoría no advierte el tipo de tecnologías digitales que son empleadas para llevar a cabo las actividades que se regulan.

9.2 Protección de datos: 2 proyectos de ley, 1 ley

Se trata de iniciativas que regulan el tratamiento de datos en la propaganda electoral, que crea la autoridad de protección de datos personales, y la que fue sancionada recientemente trata sobre las normas de identificación nacional.

El balance general de la caracterización del contenido de las iniciativas es el siguiente:

- *Mecanismos de protección*. Solo 1 proyecto de ley especifica la existencia de mecanismos de protección de tipo administrativo.
- *Derechos que reconoce.* En 2 proyectos de ley, se reconoce el ejercicio de los derechos ARCO a los titulares de los datos.
- *Datos sensibles.* En general, no determinan nada al respecto. Solo la Ley de Identificación Nacional prevé la autorización al tratamiento de datos sensibles por regla general.
- *Tecnologías digitales.* En la Ley de Identificación, se determina el uso de sistemas de autenticación o verificación biométrica.
- *Flujo transfronterizo de datos.* Solo 1 proyecto de ley contiene estándares en este sentido que refieren al nivel "suficiente" de protección.
- *Excepciones en su aplicación.* Ninguna iniciativa tiene previsiones en este sentido.
- *Privacidad por diseño y por defecto.* Ninguna iniciativa tiene previsiones en este sentido.
- *Autoridad de protección.* En 1 proyecto de ley, se crea la autoridad de protección de datos; en la ley, se delega su contenido en otras autoridades; y, en el otro proyecto de ley, no se especifica qué autoridad es competente sobre su contenido.
- Facultades de la autoridad. En 1 proyecto de ley, se prevén las facultades de investigación, vigilancia y sanción; en otro proyecto no se detallan; y, en la ley sancionada recientemente, se consagran otras facultades (remisión de datos personales al Banco de la Nación).

VII. Conclusiones

Este informe apuntó a ofrecer un primer acercamiento metodológico y de análisis general de la actividad legislativa de nueve países de la región en los últimos tres años, en materia de privacidad y protección de datos. Hay que decir que, pese a tratarse de países de una misma región que comparten una visión del derecho común (continental o civil law), ello no facilita, como vimos antes, el ejercicio de comparación legislativa en tanto que la técnica y la transparencia legislativa en cada país resulta dispar. No obstante, los ejercicios de comparación normativa permiten, con sus dificultades, medir el nivel de progreso o retroceso en dos agendas con compromisos en derechos humanos todavía pendientes. Dichos compromisos, según el análisis regional y por países, se dirigen, en general, a la necesidad de seguir armonizando la legislación de cada país con los estándares del SIDH.

En materia de protección de datos, esta es una tarea que, pese a que se refleja mejor en algunas de las más recientes iniciativas legislativas de tipo general para regular la protección de datos (como sucedió recientemente en Ecuador o Brasil), no ha logrado aún extenderse a las iniciativas de los regímenes especiales incluso al interior de una misma jurisdicción (tal y como sucede en Chile, Perú, México y Paraguay). La dispersión regulatoria de la protección de datos –que es tratada por las autoridades legislativas en iniciativas de tipo diverso según ciertas actividades, sectores económicos, tecnologías digitales o tipos de datos, por ejemplo– debe poder estar en sintonía con la Ley General de Protección de Datos (de haberla) para evitar eventos como los que se advierten a simple vista en la revisión por países; en proyectos con vacíos, lagunas o posibles antinomias (como sucede, por ejemplo, con las iniciativas de derecho al olvido en México); o en las iniciativas sobre explotación de datos biométricos en Perú.

Todavía sigue siendo preocupante que existan países en la región que no cuenten con leyes generales de protección de datos, como Paraguay, o que ni siquiera estén pensando en tramitar una, como Guatemala. Pese a que cuentan con regulación de alcance específico sobre la materia (como el sector financiero), se precisan garantías aplicables de manera indistinta al tipo de responsable, al tipo de dato o al titular, que permitan a este último la realización plena del ejercicio del control sobre su información. Ahora, los temas que parecen importar más a los nueve países –que van desde la regulación de la protección de datos en el sector financiero; el ejercicio de la protección de datos durante la emergencia sanitaria; el uso de tecnologías biométricas; hasta la regulación del ejercicio en internet– necesitan una mirada comprehensiva de su posible impacto a otros derechos, como la libertad de expresión y el

acceso a la información, así como una consideración de los estándares que rigen actualmente sus discusiones cuando se trata de su ejercicio en línea.

En materia de privacidad, el panorama de progreso de la agenda es menos optimista, si se la compara con las deudas pendientes que se advirtieron a inicios de la década pasada. La brecha entre los estándares del SIDH y el contenido de las iniciativas en trámite –y aquellas otras ya vigentes que apuntan, por ejemplo, a regular aspectos como la vigilancia individualizada o masiva– se muestra mucho más profunda. Persiste un interés, casi común en los países legislativamente activos, por ampliar la facultad de vigilancia individualizada de las comunicaciones, (incluidas o reconocidas las prácticas que, según el balance de inicio de década, son más bien viejas).

Esta disparidad entre el reconocimiento legislativo y la capacidad material de vigilar las comunicaciones de las personas que tienen las autoridades de los Estados, pese a que ya había sido advertida, y pese a los escándalos en algunos de los países analizados que cada tanto recuerdan cuán fácil es abusar de los sistemas de vigilancia, aún no han activado procesos de discusión legislativa modelo en ningún país de la región. La situación de rompecabezas legislativo todavía continúa y refleja problemas de técnica legislativa que no son propios de los temas de privacidad (y tampoco de protección de datos), que hablan de la importancia que tiene una discusión menos visible, aunque igualmente importante: la de la profesionalización de los equipos legislativos, de sensibilización y entrenamiento sobre las dificultades y los retos de la regulación de la vigilancia de las comunicaciones, entre otros.

Seguir adelante con el monitoreo de iniciativas legislativas es una tarea que permitirá contribuir a este proceso de sensibilización gracias a la visión comparada que dicho trabajo provee. Para ello, es importante considerar que, con el tiempo, la base metodológica propuesta deberá actualizarse para que los criterios de caracterización se acerquen mejor al detalle de cada iniciativa. Dicha actualización dependerá de la mejora que se precisa en torno a los procesos de transparencia legislativa en los Congresos de los países, entre otras cuestiones.

Por último, es necesario resaltar la importancia que tiene emprender estos ejercicios para las personas interesadas y las organizaciones de la sociedad civil de la región que se dedican al trabajo, a la investigación y a la incidencia en materia de protección de datos y privacidad. Este trabajo, que amplía el interés del Observatorio Legislativo del CELE, no solo provee de información de base, con capacidad comparativa para facilitar esos procesos, sino que también puede servir como punto de encuentro para la reflexión sobre las tendencias de la región y las mejores prácticas legislativas para superar la brecha entre la práctica y su regulación.

VIII. Anexos

1. Argentina

Criterios generales	Marco regulatorio	Año	Texto normativo
¿Cómo se reconoce el derecho a la protección de datos y privacidad en la Constitución política?	Constitución política	1994	Artículos 18, 19 y 43[95]
PROTECCIÓN DE DATOS			
¿Tiene Ley General de Protección de Datos?	Ley N° 25.326	2000	Ley de Protección de los Datos Personales
¿Tiene una autoridad de protección de datos?	Ley N° 27.275	2016	Agencia de Acceso a la Información Pública
¿Tiene un mecanismo de defensa?	Ley N° 25.326	2000	La acción de protección de los datos personales o de habeas data[96]
PRIVACIDAD			
¿La orden de acceso a los datos de las comunicaciones se somete a revisión judicial?	Ley N° 27.063	2019	Judicial, previa[97] Judicial, previa[98]
	Ley N° 25.520	2001	Judicial, previa y posterior[99]
¿Cuáles son las autoridades facultadas para emitir órdenes de acceso a los datos de las comunicaciones?	Ley N° 27.063	2019	Ministerio Público Fiscal en las investigaciones penales[100]
	Ley N° 25.520	2001	Agencia Federal de Inteligencia, a través de su Director General[101]
	Resolución N° 5	2013	La Comisión Nacional de Comunicaciones[102]

[95] "Toda persona puede interponer acción expedita y rápida de amparo, siempre que no exista otro medio judicial más idóneo, contra todo acto u omisión de autoridades públicas o de particulares, que en forma actual o inminente lesione, restrinja, altere o amenace, con arbitrariedad o ilegalidad manifiesta, derechos y garantías reconocidos por esta Constitución, un tratado o una ley. En el caso, el juez podrá declarar la inconstitucionalidad de la norma en que se funde el acto u omisión lesiva", art. 43.

[96] Ley de Protección de los Datos Personales, ley N° 25.326, arts. 16, 33, 34 y 37.

[97] Código Procesal Penal Federal, art. 150, interceptación. La interceptación de las comunicaciones puede tener lugar siempre que sea útil para la verificación del delito. Es una medida excepcional.

[98] Código Procesal Penal Federal, art. 151, incautación de datos.

[99] Ley de Inteligencia Nacional, arts. 18 y 19.

[100] Código Procesal Penal Federal, arts. 150 y 152.

[101] Ley de Inteligencia Nacional, arts. 5 bis, 15 bis y 18.

[102] Ministerio de Planificación Federal, Inversión Pública y Servicios, Secretaría de Comunicaciones, resolución N° 5/2013, disponible en: http://servicios.infoleg.gob.ar/infolegInternet/anexos/215000-219999/216915/norma.htm, último acceso: 13 de abril de 2022.

2. Brasil

Criterios generales	Marco regulatorio	Año	Texto normativo
¿Cómo se reconoce el derecho a la protección de datos y privacidad en la Constitución política?	Constitución política	1988	Artículo 5, numeral 71[103]
PROTECCIÓN DE DATOS			
¿Tiene Ley General de Protección de Datos?	Ley N° 13.709	2018	Ley General de Protección de Datos Personales
¿Tiene una autoridad de protección de datos?	Ley N° 13.853	2019	Autoridad Nacional de Protección de Datos
¿Tiene un mecanismo de defensa?	Constitución política	1988	Habeas data[104]
PRIVACIDAD			
¿La orden de acceso a los datos de las comunicaciones se somete a revisión judicial?	Ley N° 9.296	1996	Judicial, previa[105]
¿Cuáles son las autoridades facultadas para emitir órdenes de acceso a los datos de las comunicaciones?	Ley N° 12.830	1993	i) el Jefe de la policía civil (delegado de policía); ii) fiscales; y iii) jueces[106]
	Decreto ley N° 3.689	1941	Comisiones parlamentarias de investigación, constituidas temporalmente dentro del Poder Legislativo[107]

[103] Art. 5, num. 10. Son inviolables la intimidad, la vida privada, el honor y la imagen de las personas, asegurándose el derecho a indemnización por el daño material o moral derivado de su violación.

[104] Art. 5, num. 71. Se concederá *habeas data*: 1. para asegurar el conocimiento de informaciones relativas a la persona del impetrante que consten en registros o bancos de datos de entidades gubernamentales o de carácter público; 2. para la rectificación de datos, cuando no se prefiera hacerlo por procedimiento secreto, judicial o administrativo.

[105] Ley N° 9.296/1996, arts. 2, 4, § 2 y art. 5. y el Código de Procedimiento Penal, art. 240, §§ 1 y 2.

[106] Ley N° 12.830/2013, art. 2, § 2. Prevé la investigación criminal realizada por el jefe de policía.

[107] Código de Procedimiento Penal, art. 156 y la ley N° 9.296/1996, art. 3.

3. Chile

Criterios generales	Marco regulatorio	Año	Texto normativo
¿Cómo se reconoce el derecho a la protección de datos y privacidad en la Constitución política?	Constitución política	1980	Artículo 19, numeral 4[108]
PROTECCIÓN DE DATOS			
¿Tiene Ley General de Protección de Datos?	Ley N° 19.628	1999	Protección de la vida privada[109]
	Ley N° 21.096	2018	Consagra el derecho a la protección de datos personales[110]
¿Tiene una autoridad de protección de datos?	Ley N° 20.285	2008	Consejo para la Transparencia[111]
¿Tiene un mecanismo de defensa?	Constitución política	1980	Acción de protección[112]
	Ley N° 19.628	1999	Acción de habeas data
PRIVACIDAD			
¿La orden de acceso a los datos de las comunicaciones se somete a revisión judicial?	Código Procesal Penal. Ley N° 19.696	2000	Judicial, previa[113]
	Ley N° 18.314	1984	Judicial, previa[114]
	Ley N° 19.974	2004	Judicial[115]

Continúa...

[108] "La Constitución asegura a todas las personas: (…) 4° El respeto y protección a la vida privada y a la honra de la persona y su familia", art. 19.

[109] Esta ley estableció la forma y las condiciones bajo las cuales se pueden tratar dichos datos.

[110] Estableció que toda persona tiene derecho a la protección de sus datos personales y que el tratamiento y la protección de estos datos se efectuará en la forma y las condiciones que determine la ley.

[111] Sobre acceso a la información pública. Ley N° 20.285/2008, art. 33.

[112] Constitución política de 1980, art. 20.

[113] Código Procesal Penal, ley N° 19.696/2000, art. 222. La interceptación solo está permitida para investigar a sospechosos que hayan participado en un acto punible que ordena una pena de delito. Autorización judicial previa, art. 9.

[114] Ley N° 18.314/1984, determina conductas terroristas y fija su penalidad. Art. 14, autoriza la interceptación y la grabación de teléfonos y comunicaciones electrónicas y el acceso a la correspondencia de la persona investigada por decisión judicial motivada durante la audiencia que formalice una investigación, o una vez formalizada, cuando se aplica una medida de prisión preventiva.

[115] Ley N° 19.974/2004 sobre el sistema de inteligencia del Estado y crea la Agencia Nacional de Inteligencia, arts. 23, 24, 25.

¿Cuáles son las autoridades facultadas para emitir órdenes de acceso a los datos de las comunicaciones?	Ley N° 19.974	2004	Órganos que forman parte del Sistema de Inteligencia del Estado:[116] Agencia Nacional de Inteligencia, la Inteligencia de Defensa Dirección del Estado Mayor de la Defensa Nacional (Dirección de Inteligencia de Defensa del Estado Mayor de la Defensa Nacional), las Direcciones de Inteligencia de las Fuerzas Armadas (Direcciones de Inteligencia de las Fuerzas Armadas), y las Direcciones de Inteligencia o Jefatura de Policía y Seguridad Pública[117] (Direcciones o Jefaturas de Inteligencia de las Fuerzas de Orden y Seguridad Pública) Carabineros y Policía de Investigaciones del país, como se definió anteriormente. Los directores o los jefes de los órganos del Sistema de Inteligencia del Estado
	Código Procesal Penal. Ley N° 19.696	2000	Los fiscales[118]
	Decreto ley N° 211[119]	1973	El Fiscal Nacional Económico (Fiscal Nacional Económico)[120]

[116] Ley N° 19.974/2004, art. 25.

[117] Ley N° 19.974/2004, art. 22. La ley establece que la función de inteligencia policial corresponde exclusivamente a la de Chile.

[118] Código Procesal Penal, ley N° 19.696/2000, arts. 218 y 219. Los fiscales se consideran autoridades competentes que pueden solicitar el acceso a direcciones IP retenidas, números IP de suscriptores y registros de conexión; datos obtenidos a través de la solicitud de acceso a las copias de las empresas; o versiones de lo transmitido o comunicaciones recibidas.

[119] Decreto ley N° 211, fija normas para la defensa de la libre competencia, art. 39.

[120] Responsable de la realización de investigaciones administrativas para garantizar la libre competencia. También puede requerir el acceso a los datos de las comunicaciones al ministro de la Corte de Apelaciones de la ciudad de Santiago, al disponer que el Tribunal de Defensa de la Libre Competencia de Chile haya dado su aprobación previa. La solicitud puede incluir la interceptación de todo tipo de comunicaciones y acceso a contenidos de comunicaciones almacenados.

4. Colombia

Criterios generales	Marco regulatorio	Año	Texto normativo
¿Cómo se reconoce el derecho a la protección de datos y privacidad en la Constitución política?	Constitución política	1991	Artículo 15[121]
PROTECCIÓN DE DATOS			
¿Tiene Ley General de Protección de Datos?	Ley N° 1.581	2012	Ley estatutaria por la cual se dictan disposiciones generales para la protección de datos personales[122]
¿Tiene una autoridad de protección de datos?	Ley N° 1.581	2021	Delegatura de Protección de datos de la Superintendencia de Industria y Comercio[123] (artículo 19)
¿Tiene un mecanismo de defensa?	Constitución política	1991	Judicial[124]
	Ley N° 1.581	2012	Administrativo[125]
PRIVACIDAD			
¿La orden de acceso a los datos de las comunicaciones se somete a revisión judicial?	Ley N° 906	2004	Judicial, previa[126] Judicial, posterior[127]
¿Cuáles son las autoridades facultadas para emitir órdenes de acceso a los datos de las comunicaciones?	Ley N° 906	2004	Fiscalía General de la Nación[128] Todas las que autoridades con facultades permanentes de policía judicial,[129] y las autoridades con facultades de policía judicial en relación con sus competencias[130]

[121] "Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, *tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.* En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución. La correspondencia y demás formas de comunicación privada son inviolables. Solo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley. Para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado, podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley", Constitución política, art. 15 (la cursiva es de las autoras).

[122] Reglamento, además, por el decreto N° 1.377/2013.

[123] Ley N° 1.581/2012, art. 19.

[124] Constitución política, acción de tutela o amparo, art. 86.

[125] Ley N° 1.581/2012, prevé la petición, la consulta, la queja y el bloqueo temporal de datos.

[126] Código de Procedimiento Penal, art. 235. La orden de prórroga se somete a control previo de legalidad del juez de control de garantías.

[127] Código de Procedimiento Penal, art. 237. La orden inicial de interceptación a las comunicaciones se somete a control de legalidad posterior.

[128] Código de Procedimiento Penal, arts. 235 y ss. Se faculta a la Fiscalía General de la Nación y a "otras autoridades competentes".

[129] Ley N° 1.453/2011, art. 52, Fiscalía General de la Nación, policía judicial, GAULA.

[130] Contraloría General de la República, Fiscalía General de la Nación, DIAN, Procuraduría General de la Nación.

5. Ecuador

Criterios generales	Marco regulatorio	Año	Texto normativo
¿Cómo se reconoce el derecho a la protección de datos y privacidad en la Constitución política?	Constitución política	2008	Artículo 66, numeral 19[131]
PROTECCIÓN DE DATOS			
¿Tiene Ley General de Protección de Datos?	Registro Oficial - Quinto suplemento N° 459	2021	Ley Orgánica de Protección de Datos Personales
¿Tiene una autoridad de protección de datos?	Ley Orgánica de Protección de Datos Personales	2021	Autoridad Nacional de Protección de Datos Personales[132]
¿Tiene un mecanismo de defensa?	Constitución política	2008	Acción de habeas data[133]
PRIVACIDAD			
¿La orden de acceso a los datos de las comunicaciones se somete a revisión judicial?	Código Orgánico Integral Penal	2014	Judicial, previa[134]
¿Cuáles son las autoridades facultadas para emitir órdenes de acceso a los datos de las comunicaciones?	Código Orgánico Integral Penal	2014	Fiscal[135]

[131] "El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley", Constitución política, art. 66, num. 19.

[132] Ley Orgánica de Protección de Datos Personales, cap. XII, art. 75 y ss.

[133] Constitución política, art. 92. Acción de *habeas data*.

[134] Código Orgánico Integral Penal, art. 476, solicitud previa de la interceptación de comunicaciones; art. 477, reconocimiento de grabaciones.

[135] *Ibíd*.

6. Guatemala

Criterios generales	Marco regulatorio	Año	Texto normativo
¿Cómo se reconoce el derecho a la protección de datos y privacidad en la Constitución política?	Constitución política	1993	Derecho a la intimidad[136] Derecho a la autodeterminación informativa[137]
PROTECCIÓN DE DATOS			
¿Tiene Ley General de Protección de Datos?	Decreto N° 57/2008	2008	Al parecer, no hay Ley General sobre Protección de Datos. Pero tienen la Ley de Acceso a la Información Pública
¿Tiene una autoridad de protección de datos?	Decreto N° 57/2008	2008	Procurador de los Derechos Humanos[138]
¿Tiene un mecanismo de defensa?	Decreto N° 57/2008	2008	Acción de habeas data[139]
PRIVACIDAD			
¿La orden de acceso a los datos de las comunicaciones se somete a revisión judicial?	Código Procesal Penal	1992	Judicial, previa[140]
	Ley Control del Crimen Organizado	2006	Judicial, previa[141]
	Ley de la Dirección General de Inteligencia Civil	2005	Judicial, previa[142]
¿Cuáles son las autoridades facultadas para emitir órdenes de acceso a los datos de las comunicaciones?	Ley Contra la Delincuencia Organizada	2009	Únicamente podrá hacerse por fiscales del Ministerio Público[143]

[136] Constitución política, art. 23, inviolabilidad de la vivienda; "La correspondencia de toda persona, sus documentos y libros son inviolables", art. 24, inviolabilidad de correspondencia, documentos y libros; art. 25, registro de personas y vehículos. Establece la obligación de guardar respeto a la dignidad, la intimidad y el decoro de las personas ante los registros personales.

[137] "Toda persona tiene el derecho de conocer lo que de ella conste en archivos, fichas o cualquier otra forma de registros estatales, y la finalidad a que se dedica esta información, así como a corrección, rectificación y actualización. Quedan prohibidos los registros y archivos de filiación política, excepto los propios de las autoridades electorales y de los partidos políticos", Constitución política, art. 31, acceso a archivos y registros estatales.

[138] Parece ser que no hay una autoridad reguladora sobre la protección de los datos personales. Este decreto nos describe la intervención de los procuradores de derechos humanos en el art. 46.

[139] Decreto N° 57/2008, cap. VI, art. 30 y ss.

[140] Código Procesal Penal, arts. 203, 204, 205.

[141] Ley Contra la Delincuencia Organizada, arts. 18 y 48.

[142] Ley de la Dirección General de Inteligencia Civil, art. 4, inteligencia y contrainteligencia.

[143] Ley Contra la Delincuencia Organizada, Congreso de la República de Guatemala (2009), arts. 49 y 52. En relación a la interceptación.

7. México

Criterios generales	Marco regulatorio	Año	Texto normativo
¿Cómo se reconoce el derecho a la protección de datos y privacidad en la Constitución política?	Constitución política	1917	Artículo 16[144]
PROTECCIÓN DE DATOS			
¿Tiene Ley General de Protección de Datos?	Diario Oficial de la Federación del 5 de julio de 2010	2010	Ley Federal de Protección de Datos Personales en posesión de los particulares
	Diario Oficial de la Federación del 26 de enero de 2017	2017	Ley General de Protección de Datos Personales en posesión de sujetos obligados
¿Tiene una autoridad de protección de datos?	Ley General de Protección de Datos Personales en posesión de sujetos obligados	2017	El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales[145]
¿Tiene un mecanismo de defensa?	Constitución política	1917	Artículo 6, literal A[146]
PRIVACIDAD			
¿La orden de acceso a los datos de las comunicaciones se somete a revisión judicial?	Código Nacional de Procedimientos Penales	2014	Judicial, previa[147]
	Ley de la Guardia Nacional	2019	Judicial, previa y posterior[148]

[144] "Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros", Constitución política, art. 16, § 2.

[145] Ley General de Protección de Datos Personales en posesión de sujetos obligados, tit. VIII, cap. I. Organismos garantes del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

[146] Al parecer, no están regulados los mecanismos de protección ante una vulneración a los datos personales o privacidad. Se encontró el art. 20 de la Constitución política donde se desarrolla un proceso penal acusatorio en el que se penaliza y se resguarda "su identidad y otros datos personales en los siguientes casos: cuando sean menores de edad; cuando se trate de delitos de violación, secuestro o delincuencia organizada; y cuando a juicio del juzgador sea necesario para su protección, salvaguardando en todo caso los derechos de la defensa".

[147] Código Nacional de Procedimientos Penales, arts. 292 y 294.

[148] Ley de la Guardia Nacional. Judicial posterior, arts. 100, 101, 103 y 104. Judicial previa, art. 9, fracción XXVI.

8. Paraguay

Criterios generales	Marco regulatorio	Año	Texto normativo
¿Cómo se reconoce el derecho a la protección de datos y privacidad en la Constitución política?	Constitución política	1992	Derecho a la intimidad[149] Del derecho a la inviolabilidad del patrimonio documental y la comunicación privada[150]
PROTECCIÓN DE DATOS			
¿Tiene Ley General de Protección de datos?	--	--	No tiene LPDP, pero sí una ley que regula el tratamiento de la información
	Ley N° 1.682	2001	Reglamenta la información de carácter privado
	Ley N° 1.969	2002	Modifica, amplía y deroga varios artículos de la ley N° 1.682/2001 "que reglamenta la información de carácter privado"
¿Tiene una autoridad de protección de datos?	--	--	No tiene[151]
¿Tiene un mecanismo de defensa?	Constitución política	1992	Artículo 135, habeas data[152]
PRIVACIDAD			
¿La orden de acceso a los datos de las comunicaciones se somete a revisión judicial?	Ley N° 1.286	1998	Judicial, previa[153]
	Ley N° 5.241	2014	Judicial, previa[154]
	Ley N° 4.868	2013	Administrativo[155]
¿Cuáles son las autoridades facultadas para emitir órdenes de acceso a los datos de las comunicaciones?	Ley N° 1.286	1998	Fiscales[156]
	Ley N° 1.881	2002	La Secretaría Nacional Antidroga (SENAD)[157]
	Decreto N° 12.515	1996	La Secretaría de Inteligencia Nacional[158]

[149] "La intimidad personal y familiar, así como el respeto a la vida privada, son inviolables", Constitución política, art. 33.

[150] "El patrimonio documental de las personas es inviolable", Constitución política, art. 36, del derecho a la inviolabilidad del patrimonio documental y la comunicación privada.

[151] "Paraguay no cuenta con una ley integral de protección de datos, y la ley 1.682/2001, de información, no ha establecido una autoridad de aplicación. Como consecuencia, hay violaciones de datos. Los derechos de los sujetos previstos en esta ley podrán ser atendidos mediante denuncia a órganos administrativos de protección al consumidor o pueden ser abordados en los tribunales", Informe Global Comparativo de Electronic Frontier Foundation.

[152] "Toda persona puede acceder a la información y a los datos que sobre sí misma, o sobre sus bienes, obren en registros oficiales o privados de carácter público, así como conocer el uso que se haga de los mismos y de su finalidad. Podrá solicitar ante el magistrado competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectaran ilegítimamente sus derechos", Constitución política, art. 135.

[153] Código de Procedimiento Penal, art. 200, intervención de comunicaciones. Establece que es una excepción la medida.

[154] Ley del Sistema de Inteligencia, ley N° 5.241, art. 3, num. 4. Donde indica que "todo procedimiento y acción del Sistema Nacional de Inteligencia (SINAI) para la solicitud de información privada, deberá contar con la autorización judicial previa del órgano jurisdiccional competente" y art. 26, sobre autorización judicial.

[155] Ley de Comercio Electrónico, ley N° 4.868/2013, arts. 2, lit. f y 10. En relación con los metadatos y el acceso a los datos de conexión y tráfico de internet.

[156] Código Procesal Penal, arts. 200, 316 y 318.

[157] Ley N° 1.881 que modifica la ley N° 1.340 del 22 de noviembre de 1988 "que reprime el tráfico ilícito de estupefacientes y drogas peligrosas y otros delitos afines y establece medidas de prevención y recuperación de farmacodependientes", art. 88.

[158] Prevé la creación del Servicio de Inteligencia Dirección bajo la autoridad del Secretario de Interior (conocido como "Ministerio del Interior"), como una de las agencias incluidas en el SINAI.

9. Perú

Criterios generales	Marco regulatorio	Año	Texto normativo
¿Cómo se reconoce el derecho a la protección de datos y privacidad en la Constitución política?	Constitución política	1993	Artículo 2, numerales 6, 7, 10[159]
PROTECCIÓN DE DATOS			
¿Tiene Ley General de Protección de Datos?	Ley N° 29.733	2011	Ley de Protección de Datos
¿Tiene una autoridad de protección de datos?	Ley N° 29.733	2011	Autoridad Nacional de Protección de Datos Personales[160]
¿Tiene un mecanismo de defensa?	Constitución política	1993	La Acción de Hábeas Data[161]
PRIVACIDAD			
¿La orden de acceso a los datos de las comunicaciones se somete a revisión judicial?	Ley N° 27.697	2001	Judicial, previa[162]
	Código Procesal Penal	2004	Judicial, previa[163]
¿Cuáles son las autoridades facultadas para emitir órdenes de acceso a los datos de las comunicaciones?	Código Procesal Penal	2004	Fiscales penales, procuradores generales y fiscal nacional[164]

[159] "Toda persona tiene derecho: (…) 6. A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar. 7. Al honor y a la buena reputación, a la intimidad personal y familiar, así como a la voz y a la imagen propias. (…) 10. Al secreto y a la inviolabilidad de sus comunicaciones y documentos privados", Constitución política, art. 2.

[160] Ley de Protección de Datos, art. 32, órgano competente y régimen jurídico.

[161] Constitución política, art. 200, num. 3. La Acción de Hábeas Data, que procede contra el hecho u omisión, por parte de cualquier autoridad, funcionario o persona, que vulnera o amenaza los derechos a los que se refiere el art. 2, ins. 5 y 6 de la Constitución.

[162] Ley N° 27.697. Ley que otorga facultad al fiscal para la intervención y control de comunicaciones y documentos privados en caso excepcional, art. 2.

[163] Código Procesal Penal, art. 230. Establece que la solicitud que el fiscal remite al juez debe estar motivada y contener todos los datos necesarios.

[164] Código Procesal Penal, art. 226. La intervención de las comunicaciones solo puede ser solicitada por los fiscales penales, procuradores generales y fiscal nacional. La interceptación de comunicaciones es realizada por personal autorizado del Ministerio Público o de la p olicía n acional bajo la supervisión del fiscal encargado de la investigación.