Big Data

Análisis comparado sobre estándares regulatorios a nivel regional

Argentina unida

Jefatura de Gabinete de Ministros
Argentina

Secretaría de Innovación Pública

Índice de contenido

Introducción	3
¿Qué entendemos por Big Data?	4
Recomendaciones de la UIT para Big Data	6
Iniciativas de Big Data en la Argentina y en el resto de las Américas	8
Big Data en el continente americano. Tratamiento de datos personales	11
Transferencia internacional de datos	18
Reseñas bibliográficas	20

Introducción

En el marco del **Observatorio Nacional de Big Data**, la **Subsecretaría de Tecnologías de la Información y las Comunicaciones** (SSTIC), dependiente de la Secretaría de Innovación Pública de la Jefatura de Gabinete busca promover el intercambio de investigaciones y propuestas vinculadas con la responsabilidad de los intermediarios de internet, el tratamiento de los datos personales en entornos digitales y los impactos socioeconómicos derivados en el uso de tecnologías de procesamiento automatizado de la información.

Para ello, la **SSTIC** se propone como líder de la mesa de debate entre los organismos internacionales, las instituciones académicas, el sector privado y la sociedad civil con el objetivo de promover la discusión en torno a la evolución de las tecnologías de Big Data en la Argentina.

El presente documento representa un benchmark sobre los estándares regulatorios de la región de América Latina vinculados con las tecnologías de Big Data. En la primera parte de este trabajo se aborda la definición de Big Data y sus beneficios para el desarrollo de políticas públicas. En ese contexto, también se hace referencia a las recomendaciones de la **Unión Internacional de Telecomunicaciones** referidas al big data (Recommendation ITU-T Y.3600 [Big Data - Cloud computing based requirements and capabilities]).

El tercer apartado aborda las iniciativas de Big Data que se llevan adelante en **Argentina** y el resto de los **Estados del continente americano**, así como también iniciativas regionales como el proyecto **DARE de APEC** o la **Alianza del Pacífico**.

Consecuentemente, se realizó un relevamiento sobre legislaciones regionales vinculadas al tratamiento y protección de datos personales, siendo este un tema central al hablar de tecnologías de Big Data. Dentro de este apartado, también se hace referencia a la cuestión de la protección de datos de los niños, niñas y adolescentes.

Asimismo, se hace mención al reciente proyecto de ley de Ecuador del 26 de mayo de 2021, respecto de la protección de datos personales por considerarlo el último trabajo en materia regulatoria presentado por un país de la región. En el mismo se detallan los principios para el procesamiento y tratamiento de los datos personales, y se establecen las obligaciones para los operadores de telecomunicaciones.

Finalmente, se ofrece un apartado respecto de la transferencia internacional de datos, con los distintos acuerdos regionales y los países que los integran.

¿Qué entendemos por Big Data?

El big data, entendido como el uso innovador de grandes y diversas bases de datos, tiene un vasto potencial para la medición de impacto y la toma de decisiones (Rubinstein, 2012). El grupo de las Naciones Unidas para el Desarrollo Sostenible, creado en 1997, considera que el Big Data es un instrumento importante para monitorear el progreso y la toma de decisiones sobre políticas públicas en el marco de los **Objetivos de Desarrollo Sostenible** (ODS). En ese sentido, la '**Agenda 2030 para el desarrollo sostenible**' planteó la necesidad de recopilar datos para la medición de varias metas, para lo cual se requiere que los Estados miembros de **Naciones Unidas** fortalezcan sus capacidades en esa actividad (Asamblea General de las Naciones Unidas, 2015).

El Big Data suele definirse en términos de cinco 'v': volumen, variedad, velocidad, veracidad y valor (Klous, 2016)[1]

1. **Volumen:** se refiere a la enorme cantidad de datos generados. Esto implica, entre otros, desafíos en el procesamiento de la información, pues se requiere de sistemas que tengan la capacidad de efectuar esa tarea.
2. **Variedad:** las tecnologías actuales permiten la recopilación desde diversas fuentes, por fuera de las estructuras clásicas de información. Esto implica retos en la identificación de datos a ser utilizados.
3. **Velocidad:** la recolección de datos conlleva a un incremento exponencial de los insumos y de la capacidad de brindar respuesta en tiempo real.
4. **Veracidad:** la gran cantidad de información dificulta los controles sobre su calidad. La veracidad, entonces, exige que los datos reflejen de manera correcta la realidad que representan. En cuanto al proceso de recolección, existen desafíos sobre qué información es recopilada y cómo debe ser conservada.
5. **Valor:** el big data abre las puertas para los nuevos servicios y productos, y para la toma de decisiones basadas en evidencia. Por ejemplo, los datos a gran escala han traído beneficios en la optimización de servicios de salud, gasto eficiente para el mantenimiento de infraestructura, mejora en la producción agrícola y reducción de congestión del tráfico, entre otros.

Ahora bien, el procesamiento de datos a gran escala encuentra un límite en el derecho a la privacidad y la protección de datos personales (Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, 2017).

[1] Recuperado de: https://www.bitsoffreedom.nl/wp-content/uploads/Verkenning_32_Exploring_the_Boundaries_of_Big_Data.pdf#page=28

En el caso de América Latina, la protección de datos personales se centra en el concepto de habeas data, que es el derecho de toda persona a acceder a información sobre sí misma y a corregir aquella que sea errónea. De hecho, las cartas políticas de algunos Estados de la región incluyen el derecho a la protección de datos en el marco de la protección de la privacidad (Consejo Permanente de la Organización de Estados Americanos, 2012).

Las normas latinoamericanas en materia de protección de datos surgieron en dos olas: la primera, a fines del siglo XX e inicios del siglo XXI en Chile, Argentina y Paraguay. La segunda, entre finales de la década del 2000 y comienzo de la siguiente en países como Uruguay, México, Costa Rica, Perú, Nicaragua, Colombia y República Dominicana (Tobón, 2015). Según Van Hoboken, el modelo latinoamericano, reflejado en el europeo, establece un alto nivel de protección, con garantías legales amplias para los titulares de la información desde la recolección de datos y durante todas las etapas subsiguientes (2016).

Sin embargo, la protección de datos personales plantea varios retos prácticos. Según la Agenda 2030 de la ONU, el seguimiento de indicadores de desarrollo sostenible debe fundamentarse en “datos de calidad que sean accesibles, oportunos, fiables y desglosados por ingresos, sexo, edad, raza, origen étnico, estatus migratorio, discapacidad, ubicación geográfica y otras características pertinentes para los contextos nacionales” (Asamblea General de las Naciones Unidas, 2015).

Recomendaciones de la UIT para Big Data

En 2015, la Unión Internacional de Telecomunicaciones publicó un documento de recomendaciones en donde definió al Big Data como un paradigma para permitir la recopilación, almacenamiento, gestión, análisis y visualización, potencialmente bajo restricciones en tiempo real, de extensos conjuntos de datos con características heterogéneas.[2]

En esta gran cantidad de datos, a la que llamamos 'Big Data', suele haber **datos personales**[3], datos confidenciales y datos de acceso público. Ante esta situación, el **Grupo de las Naciones Unidas para el Desarrollo** (GNUD) establece que el uso de datos personales debe basarse en reglas justas y legítimas, sujeto a la implementación de regulaciones, reglas y políticas elaboradas por los miembros del **GNUD** (incluidas las políticas de privacidad y protección de datos), siendo estos: (i) adecuado consentimiento de la persona cuyos datos se utilizan, (ii) de conformidad con la ley, (iii) el cumplimiento de los mandatos de las organizaciones internacionales, (iv) otras necesidades legítimas para proteger el interés vital o superior de un individuo(s) o grupo(s) de individuos (2017, p. 4).

El documento afirma que deben emplearse los estándares más estrictos para la protección de datos en los procesos de obtención, acceso, recopilación, análisis u otros usos de datos sobre poblaciones vulnerables y personas en riesgo, niños, jóvenes o cualquier otro **dato sensible**[4] (2017).

El apartado 5° del documento establece que, los datos personales deben **des-identificarse**[5] cuando corresponda, utilizando métodos tales como la 'agregación de datos'[6], 'seudonomización'[7] o 'enmascaramiento', por ejemplo, para minimizar cualquier riesgo

---

[2] Recuperado de: https://www.itu.int/rec/T-REC-Y.3600-201511-I/es

[3] Datos personales: significa datos, en cualquier forma o medio, en relación con un objeto identificado o identificable respecto de un individuo que pueda ser identificado, directa o indirectamente, en el cual, a su vez, un individuo pueda ser identificado vinculando datos a otra información disponible.

[4] Los datos sensibles deben ser considerado como cualquier dato relacionado con (i) origen racial o étnico, (ii) opiniones políticas, (iii) asociación sindical, (iv) creencias religiosas u otras creencias de naturaleza similar, (v) salud mental o física, (vi) orientación sexual y otras actividades, (vii) la comisión o presunta comisión de cualquier delito, (viii) información respecto a procedimientos judiciales, (ix) cualquier dato financiero, (x) niños y, (xi) un individuo(s) o grupo(s) de individuos que pueda enfrentar cualquier riesgo de daño (físico, emocional o económico).

[5] Des-identificación: es el proceso en el cual, se utilizan todos los medios razonables para convertir datos personales en datos anónimos, al punto que no pueda ser rastreado y/o vinculado a un individuo(s) o grupo(s) de individuos.

[6] Agregación de datos: significa un proceso a través del cual los conjuntos de datos a nivel a individual, son combinados con un formato de este tipo para que no puedan ser rastreados o vinculados a un individuo.

[7] Seudonomización: es el proceso en el cual se modifican los datos personales mediante la eliminación o sustitución de todos los identificadores directos (ej. nombre, dirección, fecha de nacimiento, etc...) con otros identificadores únicos (números de identificación, etc...) de tal manera que aún sea posible distinguir a un individuo único en un conjunto de datos. El enmascaramiento es un tipo de seudonomización.

potencial para la privacidad, teniendo en cuenta la aparición de posibles daños asociados al uso y no-uso de datos (2017).

El acceso, análisis u otro uso de los datos debe ser coherente con la **Carta de Naciones Unidas**, y en el fomento para las metas de **Desarrollo de la Sostenibilidad**. Los datos deben ser obtenidos, recopilados y analizados a través de medios legales, legítimos y justos. En particular, el acceso a los datos, análisis y otros usos, deben cumplir con las leyes aplicables, incluyendo leyes de privacidad y protección de datos, así como los más altos estándares de confidencialidad y conducta moral y ética (UNDG, 2017)[8].

Según el '**United Nations Development Group**' (UNDG), los mecanismos adecuados de gobernanza y rendición de cuentas, deberían establecerse para monitorear el cumplimiento de la ley pertinente, incluyendo leyes de privacidad y los más altos estándares de confidencialidad, moral y conducta ética respecto al uso de los datos. En este sentido, la transparencia es un elemento fundamental de la rendición de cuentas. Esta práctica de transparencia se suele fomentar cuando los beneficios de la transparencia son mayores que los riesgos (2017).

Los datos abiertos son un importante motor de innovación, transparencia y responsabilidad. Por lo tanto, siempre que sea posible, los datos deben hacerse abiertos, a menos que los riesgos de abrir los datos sobrepasan los beneficios, o existan otras bases no legítimas para no hacerlo.

[8] Recuperado de: https://unsdg.un.org/sites/default/files/UNDG_BigData_final_web.pdf

Iniciativas de Big Data en la Argentina y en el resto de las Américas

En la última década, Argentina, Colombia, Chile y Estados Unidos han lanzado acciones específicas sobre Big Data, reconociendo tanto la creciente importancia de esta práctica para la competitividad económica futura, como las preocupaciones relacionadas. Las medidas tomadas por estos países, incluyen la promoción de servicios de big data, y el análisis de sus implicaciones regulatorias, con un enfoque particular en temas de seguridad y protección de datos. También hay iniciativas en las Américas que apuntan a la falta de desarrollo profesional específico en análisis de datos y 'IT', que parecen obstaculizar el desarrollo del concepto en la región.

A continuación, se detalla en un cuadro de columnas las distintas medidas llevadas a cabo por los países de la región con iniciativa en cuestiones referidas al uso de big data (Cullen Int., 2017)[9]:

País	Fecha	Medida	Observación
Argentina	01/06/2017	Establecimiento del 'Observatorio Nacional de Big Data' para promover y analizar las implicancias regulatorias, y crear plataformas públicas sobre big data. Los objetivos del observatorio son: 1. analizar la evolución de la tecnología de big data y las posibilidades de innovación y uso público; 2. estudiar el marco regulatorio de protección de datos en términos de big data; 3. promover y crear plataformas públicas; 4. analizar los riesgos del uso de soluciones de big data; 5. promover el uso de macrodatos en el contexto de la seguridad y en la lucha contra la delincuencia; 6. coordinar con otros ministerios relevantes (Justicia y Modernización), y con los organismos gubernamentales, provinciales y locales en temas relacionados con big data.	https://www.boletinoficial.gob.ar/detalleAviso/primera/164755/20170608

[9] Recuperado de: https://www.cullen-international.com/client/site/documents/FLECRA20170002

Colombia	22/03/2016	Establecimiento de un centro de Big Data, para que los sectores público y privado y la academia se reúnan para promover soluciones de big data y análisis de datos. Actualmente, existe la Alianza Caoba, siendo este un centro de excelencia y apropiación que apoya el uso de tecnologías de big data y data analytics[10]	https://www.dnp.gov.co/Paginas/Big-Data-Colombia-entra-en-la-revoluci%C3%B3n-de-los-datos-.aspx
Chile	15/03/2017	En 2017, la presidenta Michelle Bachelet envió un proyecto de ley de protección de datos personales. Este actualiza la ley 19.628 de 1999 con el objetivo de garantizar los derechos fundamentales y establecer principios relativos al procesamiento de datos personales. El proyecto de ley ingresó el 15 de marzo de 2017, y desde esa fecha está en primer trámite constitucional en el Senado. En julio de 2018 recibió indicaciones, y a junio de 2021 ha tenido siete urgencias, pero sigue en la Comisión de Hacienda de la Cámara Alta.[11]	https://www.cullen-international.com/client/site/documents/FLECCL20170001?version=this
Estados Unidos	01/04/2014	Fue publicado un informe de Big Data bajo la administración de Obama en 2014. El mismo incluye recomendaciones sobre inversión, investigación, ampliación y diversificación del liderazgo técnico y mayor alfabetización sobre discrimnación de datos, refuerzo de la responsabilidad y creación de estándares, para su uso en el gobierno como en el sector privado.	httprchives.gov/sites/defaults://obamawhitehouse.at/files/docs/big_data_privacy_report_may_1_2014.pdf

Fuente: **Elaboración propia[12].**

Asimismo, también existen otras iniciativas regionales para fomentar y ayudar al desarrollo de Big Data en la región (Cullen Int., 2017):

Iniciativa regional	Fecha	Medida	Observación
Proyecto DARE de	01/06/2017	El proyecto busca abordar la escasez actual de empleados capacitados en	https://www.apec.org/Press/Infographics/10%20Rec

[10] Para más información: https://www.alianzacaoba.co/nosotros
[11] Recuperado de: https://www.fintechile.org/noticias/claves-para-entenderel-retraso-del-proyecto-de-ley-de-proteccion-de-datos-personales
[12] El Ministerio de Comunicaciones de Argentina y el Ministerio de TIC de Colombia han acordado compartir información sobre sus iniciativas de IoT y Big Data.

APEC (Data Analytics Raising Employment)		ciencia de datos y análisis, desarrollando un conjunto de diez Competencias recomendadas de APEC Data Science y Analytics para servir como un recurso para equipar instituciones académicas y proveedores de capacitación en Economías de APEC para alinear planes de estudio, cursos y programas para llenar la brecha entre las habilidades y la demanda de empleadores.	ommended%20APEC%20Data%20Science%20and%20Analytics.aspx
Alianza del Pacífico	30/06/2017	Actualmente bajo liderazgo del Gobierno de Colombia, acordó compartir experiencias relacionadas con su observatorio de economía digital y su plataforma de base de datos abierta, y otorgar becas para carreras tecnológicas.	https://www.cullen-international.com/client/site/documents/FLECRA20170001?version=this

Fuente: **Elaboración propia en base a los datos de Cullen Internacional.**

Big Data en el continente americano. Tratamiento de datos personales

La región no tiene una ley homogénea sobre protección de datos personales como es el caso de la **Unión Europea** que posee el **Reglamento General de Protección de Datos Personales** que entró en vigor el 25 de mayo de 2018, (Comisión de la Comunidad Europea, 2003), tal como figura en el documento "**Estándares para una Internet Libre, Abierta e Incluyente**", elaborado por la **Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos**[13].

En 1999, Chile fue uno de los primeros países de América Latina con una ley de protección de datos. Luego, en el año 2000 Argentina aprobó la Ley 25.326, con la cual posiciona al país con una legislación que incluye un Registro Nacional de Bases De Datos, un órgano de control y una adecuación aprobada, el 30 de junio de 2003, con arreglo a la directiva 95/46/CE del Parlamento Europeo y del Consejo sobre la adecuación de la protección de los datos personales en Argentina (Vilan & Bosque, 2018).

En agosto de 2018, el Parlamento de Brasil aprobó la normativa **LGPD** como Ley N° 13.709, desde entonces la ley se ha modificado dos veces y entró en vigor el 15 de agosto de 2020. En este caso, propone que la legislación sea aplicable a empresas que tienen sede en dicho país y realicen recolección de datos en el territorio brasileño. Además de requerir el consentimiento del ciudadano para el tratamiento de los datos, también se deben brindar las herramientas para que el usuario de los datos pueda acceder, corregir o eliminar toda la información. En caso de incumplimiento de la norma, se estima que las sanciones incluyen multas altas como el 4% de los ingresos de la compañía en Brasil, limitados a 50 millones de reales. También se le prohibirá la recolección de datos y actividades de tratamiento direccionadas en Brasil (Vilan & Bosque, 2018).

Por su parte, Chile incorporó, en 2018, nuevos principios al proyecto de ley aprobado que modifica la **Ley N° 19.628**. Entre las novedades surge la modificación al alcance de datos personales, ahora se refiere a cualquier información vinculada o referida a una persona natural, identificada o identificable. A su vez, modifica el consentimiento y lo define como voluntad libre, específica, inequívoca e informada. Eliminan el consentimiento escrito (Vilan & Bosque, 2018).

De igual manera, México también endureció su normativa y en abril de 2018 se aprobó la Ley de Protección de Datos Personales en posesión de sujetos obligados. Esta ley tiene como objetivo establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales en posesión de sujetos obligados, que

[13] Recuperado de: http://www.oas.org/es/cidh/expresion/docs/publicaciones/internet_2016_esp.pdf

son considerados por ley en el ámbito estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos. El Estado garantizará la protección de datos personales de sus titulares (Vilan & Bosque, 2018).

País	Año	Fuente legal
Argentina	2000	Ley N° 25.326
Brasil	2020	Ley N° 13.709
Costa Rica	2011	Ley N° 8.968
Chile	1999	Ley N° 19.628
Colombia	2012	Ley N° 1.581
México	2010	Ley Federal de Protección de Datos Personales
República Dominicana	2013	Ley N° 172-13
Ecuador	2021	Ley orgánica de protección de datos personales

Fuente: **Elaboración propia.**

El consentimiento como fundamento para el tratamiento de datos y sus posibles alternativas

Actualmente, en el contexto digital evidenciamos diversos procesos de recolección masiva de datos que representan verdaderos desafíos frente al consentimiento. No obstante, desde la **Unión Europea** se ha planteado que el consentimiento no siempre es el fundamento más apropiado para legitimar el tratamiento de datos (United Nations Development Group, 2017). En ese contexto, se pueden plantear los siguientes criterios utilizados en países de la región que pueden ser de utilidad para el uso de datos en el marco de big data, más allá del consentimiento.

A. Cuando los datos se obtienen de fuentes de acceso público

En Argentina, la ley establece que no será necesario el consentimiento cuando "los datos se obtengan de fuentes de acceso público irrestricto" (Ley N° 25.326, 2000, art. 5.2.a.). Por su parte, la legislación de Costa Rica dispone que no se requerirá consentimiento expreso cuando "se trate de datos personales de acceso irrestricto, obtenidos de fuentes de acceso público general" (Ley N° 8.968, 2011, art. 5.2.b.). De igual modo, República Dominicana autoriza el tratamiento cuando los datos "se obtengan de fuentes de acceso público" (Ley N° 172-13, 2013, art. 27). Por último, Colombia enmarca esta autorización en términos de lo excepcional:

salvo los datos que tengan naturaleza pública, el tratamiento está sujeto a restricciones legales (Ley 1581, 2012, art. 4.h).

Esta excepción al consentimiento no exonera a la organización que hace tratamiento de cumplir con las demás obligaciones de protección de datos personales. Esta excepción al consentimiento no deroga el habeas data. En este sentido, se deben garantizar los derechos de los usuarios y se debe brindar un nivel de protección adecuado de la información. Así lo ha interpretado el Tribunal de Justicia de la Unión Europea (TJUE, 2008).

B. Cuando la finalidad es estadística, científica o histórica, siempre y cuando no se identifique al titular

La norma argentina postula que los datos sensibles "también podrán ser tratados con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares" (**Ley N° 25.326**, 2000). Aquí podemos observar que las restricciones establecidas por la ley de ese país no aplican para encuestas de opinión, estadísticas oficiales, trabajos de prospección de mercados, investigaciones científicas o médicas y actividades análogas, "en la medida que los datos recogidos no puedan atribuirse a una persona determinada o determinable" (**Ley N° 25.326**, 2000, art. 28.1). A su vez, agrega que, en caso de que no pueda mantenerse el anonimato en el proceso de recolección de datos, "se deberá utilizar una técnica de disociación, de modo que no permita identificar a persona alguna" (**Ley N° 25.326**, 2000, art. 28.1).

La ley en Colombia libera del consentimiento del titular cuando se trate de información autorizada por la ley para "fines históricos, estadísticos o científicos" (**Ley N° 1581**, 2012, art. 10). Los datos sensibles pueden tratarse excepcionalmente con esos mismos fines, pero "deberán adoptarse las medidas conducentes a la suspensión de identidad de los titulares" (**Ley N° 1581**, 2012, art. 6.e). De igual manera, la ley de Costa Rica contempla esa salvedad (**Ley N° 8969**, 2011. art. 5.2.d).

Por otro lado, la ley de República Dominicana considera que no se requerirá consentimiento en los casos en los que se haya dado un proceso de "disociación de información" que permita que los titulares no sean identificables. Según la norma, los "datos especialmente protegidos" pueden ser tratados "con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares" (**Ley N° 172-13**, 2013, arts 27.9 y 75).

C. Cuando se trata de bases de datos con fines periodísticos

Esta excepción se basa en la necesidad de que el habeas data, no anule en la práctica, el ejercicio de la libertad de expresión. Según la ley argentina, "en ningún caso se podrán afectar las bases de datos ni las fuentes de información periodísticas" (**Ley N° 25.326**, 2000, art. 1).

En Colombia, la norma exceptúa "las bases de datos y archivos de información periodística y otros contenidos editoriales" (**Ley N° 1581**, 2012, art. 2.d). Por otro lado, la ley en República Dominicana no establece nada sobre esta cuestión. La de Costa Rica apenas prevé una

garantía general para la actividad periodística al decir "en ningún caso se afectarán las fuentes de información periodísticas" (**Ley N° 8969**, 2011, art. 1).

▶ La protección de datos más allá de la autorización para recolectar

A. Cambios en la finalidad del tratamiento

La ley argentina establece que "los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención" (**Ley N° 25.326**, 2000, art. 4.3). En casi idéntico sentido está la ley dominicana (**Ley N° 172-13**, 2013, art. 56.2).

Por su parte, Costa Rica establece que cualquier uso que no sea autorizado por el titular constituirá una falta grave (**Ley N° 8969**, 2011, art. 30). En el caso de Colombia, la ley considera que hay una obligación de informar la finalidad del tratamiento (**Ley N° 1581**, 2012, art. 4.b).

B. Calidad de información

Las leyes de habeas data establecen requisitos frente a la calidad de información que reposa en las bases de datos. En principio, la norma argentina establece que los datos deben ser "ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieran obtenido" (**Ley N° 25.326**, 2000, art. 4.1).

La ley de Costa Rica contempla que, cualquier tratamiento requiere que los datos sean "actuales, veraces, exactos y adecuados al fin para el que fueron recolectados" (**Ley N° 8698**, 2011, art. 6). En términos muy similares se expresa la ley de Colombia.

En el caso de República Dominicana considera que la información debe ser "lícita, actualizada, exacta y veraz, de forma tal que responda a la situación real del titular de la información en un momento determinado" (**Ley N° 172-13**, 2013, art. 56).

C. Obligaciones de seguridad de la información y confidencialidad para los agentes que hacen el tratamiento

En el caso de Argentina, está prohibido el registro de información en bases de datos que "no reúnan condiciones técnicas de integridad y seguridad" (**Ley N° 25.326**, 2000, art. 9). En términos similares se aprecia esa obligación en República Dominicana (**Ley N° 172-13**, 2013, art. 5.5).

La ley de Costa Rica dispone que a esa obligación de seguridad se suma la implementación de "los mecanismos de seguridad física y lógica más adecuados de acuerdo con el desarrollo tecnológico actual" (**Ley N° 8969**, 2011, art. 10).

En Colombia, la norma refiere a tener las condiciones necesarias para la seguridad de la información, y, en caso de vulneraciones u otro tipo de riesgos, debe notificarse a la Superintendencia de Industria y Comercio (**Ley N° 1581**, 2012, arts. 17.d, 17.n, 18.b, 18.k).

Finalmente, en todos los Estados "se establece una obligación de secreto profesional sobre los datos tratados, incluso después de que termine su uso. Esta obligación, que se extiende más allá de aquel que abarca el uso de los datos, suele pasarse por alto" (C. Cortés y E. Vargas, 2019, p. 11).

D. Destrucción de la información con el paso del tiempo

En este contexto, las obligaciones de seguridad y confidencialidad se relacionan con el deber de destruir la información con el paso del tiempo. En general, se entiende que una vez que finalice la autorización y finalidad de uso, los datos deben destruirse (C. Cortés y E. Vargas, 2019). Sin embargo, la ley de Costa Rica establece que "en ningún caso, serán conservados los datos personales que puedan afectar, de cualquier modo, a su titular, una vez transcurridos diez años desde la fecha de ocurrencia de los hechos registrados, salvo disposición normativa especial que disponga otra cosa" (**Ley N° 8698**, 2011, art. 6.1).

▶ América del Sur y la protección de datos de los niños, niñas y adolescentes

En el caso de Chile, con la reforma de la **Ley N° 19.628**, los datos personales de niños y niñas se establecen a personas menores de 14 años, y para su recopilación se solicita una autorización de padres y adolescentes. En el caso de los adolescentes, personas menores entre 14 y 18 años, tendrán el mismo tratamiento que los adultos a excepción de sus datos sensibles que deberán ser objeto de autorización de sus padres o representantes (Vilan & Bosque, 2018, p. 7).

En el caso de Brasil, la Ley N° 13.709, posee un apartado especial sobre niños y adolescentes en la sección III, art. 14. Sostiene que el tratamiento de datos personales debe realizarse con el consentimiento específico por al menos uno de los padres o responsable legal. Además, todos aquellos que realizan tratamiento de datos de personas menores deberán mantener pública la información sobre los tipos de datos recolectados y la forma de utilización y los procedimientos para el ejercicio de los derechos de acceso (Vilan & Bosque, 2018, p. 7).

La regulación brasileña incorpora también que las empresas deben hacer esfuerzos razonables y tecnológicos para verificar la edad de los niños, niñas y adolescentes. Si bien la **Ley de Protección de Datos Personales de la Argentina** no diferencia entre el tratamiento de los datos personales de mayores y de menores de edad, la **Convención sobre los Derechos del Niño en Argentina** tiene rango constitucional y por lo tanto, carácter de ley. En dicho pacto internacional se especifica que ningún niño o niña puede ser objeto de injerencias arbitrarias o ilegales en su vida privada. Por lo tanto, se trata de un principio que se aplica para el tratamiento de datos personales de chicas y chicos en nuestro país.

El caso de Ecuador

El 26 de mayo de 2021 Ecuador publicó la nueva **Ley de Protección de Datos**, convirtiéndose en el último trabajo en materia regulatoria con fuerza de ley en un país de la región. La ley ecuatoriana incluye reglas sobre cómo los interesados pueden proteger, acceder y dar su consentimiento sobre el uso de datos personales. La normativa entraría en vigencia a partir de mayo de 2023 por lo que las empresas tienen un periodo de dos años para ajustar su proceso a las nuevas reglas.

La constitución del Ecuador reconoce el derecho a la protección de datos y la garantía constitucional del 'habeas data'. Sin embargo, no fue hasta mayo de 2021 que se aprueba una ley específica para proteger los datos personales.

En marzo de 2010, el gobierno ecuatoriano creó la **Dirección Nacional de Registro de Datos Públicos** (Dinardap) para regular, administrar y controlar el sistema de registro de datos públicos (una base de datos única de todos los registros de datos públicos del país). En este sentido, **Dinardap** debe velar por la seguridad de los datos públicos, la organización, la sistematización, la interconexión de la información y el cruce de datos, entre diferentes entidades públicas. La **Dinardap** preside el **Sistema Nacional de Registro de Datos Públicos** (Sinardap).

Inspirada en el **Reglamento General Europeo de Protección de Datos** (GDPR, Tracker), la nueva ley para la protección de datos personales en Ecuador establece principios para el procesamiento de datos personales[14]:

I. **Juridicidad:** en cuanto a que el uso de los datos depende de la existencia de disposiciones legales.
II. **Propósito:** debe haber un propósito explícito declarado para todos los datos recopilados. El uso debe limitarse a los límites indicados en el momento de la recogida de datos.
III. **Lealtad:** los propietarios de los datos deben tener una comprensión clara de por qué y cómo se recopilan, utilizan, consultan o tratan sus datos.
IV. **Transparencia:** toda la información relacionada con el procesamiento de datos debe ser accesible y fácil de entender.
V. **Relevancia:** los datos personales deben ser relevantes y estar limitados a la finalidad para la que fueron recopilados.
VI. **Proporcionalidad:** el tratamiento de los datos debe ser adecuado, necesario, oportuno, pertinente y no excesivo en relación con los fines de recogida.
VII. **Confidencialidad:** ningún procesamiento adicional de datos personales para un propósito diferente para el que se recopilaron inicialmente los datos, a menos que el propietario de los datos lo habilite explícitamente.
VIII. **Calidad y exactitud:** los datos personales tratados deben ser exactos, completos, precisos, verificables, claros y actualizados si es necesario.

[14] Recuperado de: https://www.cullen-international.com/client/site/documents/FLECEC20210001

IX. **Retención limitada:** los datos personales no deben conservarse durante un período superior al necesario para cumplir con la finalidad del tratamiento. El responsable del tratamiento establecerá plazos para su supresión o revisión periódica.
X. **Seguridad de los datos personales y responsabilidad proactiva y probada:** los controladores y procesadores de datos deben implementar todas las medidas para proteger los datos.

Asimismo, el texto legal establece obligaciones para los operadores de telecomunicaciones. En este sentido, la ley de protección de datos de Ecuador modifica algunos artículos de la **Ley de telecomunicaciones de 2015** y establece obligaciones específicas a los operadores:

I. Las redes y los sistemas deben garantizar la protección de los datos personales;
II. Los operadores no pueden utilizar datos personales con fines publicitarios o de marketing sin el consentimiento explícito del interesado;
III. Garantizar el derecho de los usuarios finales a no aparecer en los directorios telefónicos o de abonados.

En ese contexto, el regulador de las telecomunicaciones de Ecuador (Arcotel) debe implementar medidas para preservar la seguridad de la red y garantizar la protección de datos en todos sus servicios.

Transferencia internacional de datos

UE

Tanto la Argentina como Canadá y Uruguay han sido reconocidos por la Unión Europea (UE) por contar con un nivel adecuado de protección de datos personales.

En el caso de Canadá, el 20 de diciembre de 2001 la Comisión de las Comunidad Europea afirmó que "Canadá garantiza un nivel adecuado de protección de los datos personales transferidos desde la Comunidad a los receptores sujetos a la **Personal Information Protection and Electronic Documents Act** (Ley canadiense).[15]

Asimismo, el 30 de junio de 2003 la **Comisión de las Comunidad Europea** extendió esa conformidad hacia la Argentina al considerar que nuestro país "garantiza un nivel adecuado de protección por lo que respecta a los datos personales transferidos desde la Comunidad".[16]

Lo mismo sucede con Uruguay, siendo que la Comisión Europea estableció el 21 de agosto de 2012 que "la República Oriental del Uruguay garantiza un nivel adecuado de protección de los datos personales transferidos desde la Unión Europea".[17]

La relevancia de contar con este aval de la **UE** está vinculada con la entrada en vigor del **Reglamento de Protección de Datos** (conocido como GDPR), considerado el estándar más alto en la materia. El mismo establece en su Capítulo 5 mecanismos para la transmisión de datos como la adecuación de garantías mínimas para la protección de datos personales en países fuera de la **UE**. El objetivo de este apartado es permitir la transferencia internacional sólo a países con niveles de protección adecuados.

APEC

La cooperación **Económica Asia-Pacífico** (APEC) tiene dos acuerdos específicos que facilita las transferencias transfronterizas de datos personales, disponibles para los miembros de forma voluntaria (Cullen International, 2021):

- El Acuerdo de aplicación de la privacidad transfronteriza (CPEA), tiene como objetivo facilitar el intercambio de información entre las autoridades y proporcionar mecanismos de aplicación para promover una cooperación transfronteriza eficaz. La

[15] Recuperado de: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32002D0002&from=en
[16] Recuperado de: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32003D0490&from=EN
[17] Recuperado de: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32012D0484&from=EN

CPEA es un acuerdo voluntario administrado por la **Comisión Federal de Comercio de EE.UU. y el Sistema de Reglas de Privacidad Transfronterizas** (CBPR), que requiere que las políticas y prácticas de privacidad de las empresas que operan en la región **APEC**, sean evaluadas y certificadas por un verificador externo.
Aunque Chile es parte de **APEC**, entre los países monitoreados sólo Canadá, México y Estados Unidos han firmado hasta ahora tanto la **CPEA** como la **CBPR**.

▶ USMCA

El acuerdo **Estados Unidos-México-Canadá** (USMCA) incluye un capítulo de comercio digital. Este capítulo prohíbe la restricción a la transferencia transfronteriza de información personal entre los tres países, permitiendo restricciones proporcionadas como excepción para lograr un objetivo legítimo de política pública. Sólo unos pocos países son parte de acuerdos formales que permiten transferencias transfronterizas de datos personales.[18]

País	USMCA	APEC	UE
Argentina			Si
Brasil			
Canadá	Si	Si	Si
Chile			
Colombia			
Estados Unidos	Si	Si	
México	Si	Si	
Uruguay			Si

Fuente: **Elaboración propia en base a los datos de Cullen Intrl.**

[18] Recuperado de: https://www.cullen-international.com/client/site/documents/CTECLN20210039

Reseñas bibliográficas

- Rubinstein, I. (2012). Big data: the end of privacy or a new beginning?
- Asamblea General de las Naciones Unidas (Ed.). (2015). Transformar nuestro mundo: la Agenda 2030 para el Desarrollo Sostenible. A/RES/70/1. Retrieved from http://www.un.org/en/ development/desa/population/migration/generalassembly/docs/globalcompact/A_RES_70_1_E.pdf .
- Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data. (2017). Guidelines on the protection of individuals with regard to the processing of personal data in a world of big data. Retrieved from https://rm.coe.int/CoERMPublicCommonSearchServices/ DisplayDCTMContent?documentId=09000016806ebe7a
- Consejo Permanente de la Organización de Estados Americanos, Comisión de Asuntos Jurídicos y Políticos. (2012). Estudio Comparativo: Protección de Datos en las Américas. Retrieved from http://www.oas.org/es/sla/ddi/docs/ cp-cajp-3063-12.pdf
- Tobon, C. (2015). Data privacy laws in Latin America: An overview. Int'l L. News, 44.
- Van Hoboken, J. (2016). From Collection to Use in Privacy Regulation? A Forward Looking Comparison of European and U.S. Frameworks for Personal Data Processing. Van Der Sloot, Broeders and Schrijvers.
- Gutiérrez, H., & Korn, D. (2013). Facilitando the Cloud: Data Protection Regulation as a Driver of National Competitiveness in Latin America. The University of Miami Inter-American Law Review, 45(1), 33-61.
- Tribunal de Justicia de la Unión Europea (TJUE). (2008, diciembre 16). Sentencia ECLI:EU:C:2008:727.
- Estado de Argentina. (2000, octubre 4). Ley N° 25.326. Argentina.
- Estado de Colombia. (2013, septiembre 5). Decreto N° 1377. Colombia.
- Estado de Costa Rica. (2011, septiembre 5). Ley N° 8.968. Costa Rica.
- Estado de Rep. Dominicana. (2013, diciembre 15). Ley N° 172-13. República Dominicana.
- Cortés, C., & Vargas, E. (2019, febrero). Barreras legales para el big data en el marco de los Objetivos de Desarrollo Sostenible en Latinoamérica. Big Data for Development. Retrieved from https://cepei.org/wp-content/uploads/2019/10/PolicyBrief_Barreras-Legales_espa%c3%b1ol_vf-1.pdf
- Unión Internacional de Telecomunicaciones. (2015, noviembre). Recommendation ITU-T Y.3600. Retrieved from https://www.itu.int/rec/T-REC-Y.3600-201511-I/es
- Cullen International. (2017, julio 19). Big data initiatives in Argentina and elsewhere in the Americas. Retrieved from Cullen International: https://www.cullen-international.com/client/site/documents/FLECRA20170002

- Vilan, M., & Bosque, L. (2018, noviembre). Marketing Digital y protección de datos personales en la era del Big Data en América Latina. Argentina. Retrieved from https://repositorio.uade.edu.ar/xmlui/bitstream/handle/123456789/12623/C19S23%20-%20Ponencia%20%28texto%20completo%29.pdf?sequence=4&isAllowed=y
- Agencia de Acceso de Información Pública. (2017). Anteproyecto de Ley de Protección de Datos Personales. Argentina. Retrieved from http://www.jus.gob.ar/media/3223892/anteproyecto_mayo2017.pdf
- Klous, S. (2016). Sustainable Harvesting of the Big Data Potential. In Exploring the Boundaries of Big Data (pp. 25-49). Bart van der Sloot, Dennis Broeders & Erik Schrijvers (eds.). Retrieved from https://www.bitsoffreedom.nl/wp-content/uploads/Verkenning_32_Exploring_the_Boundaries_of_Big_Data.pdf#page=28
- Cullen international. (2021, junio 9). Ecuador approves data protection law. Retrieved from Cullen international: https://www.cullen-international.com/client/site/documents/FLECEC20210001
- Presidencia de la República del Ecuador. (2021, mayo 21). Ley orgánica de protección de datos personales. Quito, Ecuador. Retrieved from https://www.asambleanacional.gob.ec/sites/default/files/private/asambleanacional/filesasambleanacionalnameuid-29/Leyes%202013-2017/920-lmoreno/ro-459-5to-sup-26-05-2021.pdf
- Cullen International. (2021, febrero 12). International data transfers. Retrieved from Cullen International: https://www.cullen-international.com/client/site/documents/CTECLN20210014?version=this
- Comisión de la Comunidad Europea. (2001). Decisión de la Comisión de 20 de diciembre de 2001 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección de los datos personales conferida por la ley canadiense Personal Information and Electron. (pp. 13 - 16). Bruselas: Diario Oficial de las Comunidades Europeas.
- Comisión de la Comunidad Europea. (2012). Decisión de Ejecución de la Comisión de 21 de agosto de 2012 de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales por la República Oriental del Uruguay en lo que resp. (pp. 11 - 14). Bruselas: Diario Oficial de la Unión Europea.
- Comisión de la Comunidad Europea. (2003). Decisión de la Comisión de 30 de junio de 2003 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo sobre la adecuación de la protección de los datos personales en Argentina. (págs. 19 - 22). Bruselas: Diario Oficial de la Unión Europea.