Anuario Jurídico y Económico Escurialense, **LIX (2026) 173-200 / ISSN: 1133-3677**

La influencia del Reglamento General de Protección de Datos en la normativa de protección de datos de carácter personal en las empresas de los países latinoamericanos*

The influence of the General Data Protection Regulation on the personal data protection regulations in companies in Latin American countries

Dr. Iván MARTÍN GÓMEZ
Universidad Católica de Ávila

Resumen: El presente trabajo plantea una revisión del estado actual de la influencia generada en la legislación latinoamericana en materia de protección de datos a partir del análisis comparativo del tratamiento dado por el legislador de cada estado de los estudiados bajo el marco de los estándares establecidos por la Red Iberoamericana de Protección de datos, con el Reglamento europeo y la legislación española. Se plantean en último término unas sugerencias comunes susceptibles de ser tenidas en cuenta como ejes vertebradores de la proyección normativa necesaria de este ámbito jurídico concreto en esta zona geográfica.

Abstract: This paper reviews the current state of influence on Latin American data protection legislation based on a comparative analysis of the treatment given by the legislator of each state studied under the framework of the standards established by the Ibero-American Data Protection Network, with the European Regulation and Spanish legislation. Finally, it offers some common suggestions that could be taken into account as the backbone of the necessary regulatory framework for this specific legal area in this geographical region.

Palabras clave: Protección de datos, influencia europea, Reglamento General de Protección de Datos, Estándares iberoamericanos de protección de datos.

---

* Nota: Esta investigación se ha realizado en el marco de una estancia investigadora llevada a cabo en la ESAN *Business Law* de la Universidad ESAN en Lima (Perú), que ha resultado fundamental para el desarrollo del trabajo.

Keywords: Data protection, European influence, General Data Protection Regulation, Ibero-American data protection standards.

Sumario:

Recibido: septiembre 2025.
Aceptado: noviembre 2025.

I. INTRODUCCIÓN

En los países europeos las normativas internas de protección de datos han replicado en general las disposiciones ya establecidas por el Reglamento General de Protección de Datos (en adelante RGPD) y las remisiones al mismo son habituales tal y como sucede en nuestra norma de protección de datos. Se pretende en este estudio abordar la enorme influencia que el RGPD ha tenido en el derecho de la mayoría de los países latinoamericanos estudiados.

La doctrina consideró que resultaba necesaria la armonización jurídica de la protección de datos para un adecuado control del comportamiento de los agentes intervinientes con la Unión Europea por el intercambio existente de bienes, servicios, ciudadanos…ya que la aplicación del Reglamento europeo va más allá de su territorio[1].

Analizaremos a continuación las cuestiones más relevantes de la legislación de los principales países latinoamericanos y su comparación con el derecho europeo y español.

En algunos de ellos como son los casos de Perú, México o Chile, se han publicado recientemente normativas en esta materia que hacen mucho más interesante y actual el análisis de la protección de datos y su afectación en el sector empresarial.

Se realizará en este trabajo un estudio exploratorio-descriptivo para descubrir y prefigurar el estado de la cuestión de la protección de datos en los principales marcos regulatorios de Latinoamérica y un análisis comparativo que permita apreciar la influencia en estos ordenamientos jurídicos del RGPD y de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, (en adelante LOPDGDD).

Tras la exploración realizada se sugieren al final de este trabajo unas propuestas comunes que pueden coadyuvar al desarrollo regulatorio y que

[1] MAYORGA-JÁCOME T. C., *et al*., "Historia de la normativa reguladora de la Protección de Datos de carácter personal en distintos países Latinoamericanos", en *Revista Científica Dominio de las Ciencias*, 5 / 1 (2019) 518-537, p. 19.

pueden servir de base a futuros razonamientos jurídicos, ante la oportunidad en la que se encuentran los legisladores de estos países, debido a la incipiente armonización jurídica de la protección de datos a los estándares iberoamericanos y al Reglamento europeo, así como al resto de normas internacionales con las que cada Estado se haya comprometido. Para ello, se aplicará una recopilación de información mediante la que se describe la normativa y las observaciones de los autores expertos y más relevantes en esta materia en cada país.

A través de la investigación cualitativa que se va a realizar se trabajará en la observación de registros narrativos para lograr un análisis jurídico-comparativo de los ordenamientos estudiados con la norma de referencia en este campo del derecho: el Reglamento europeo de protección de datos y también con lo establecido en nuestra norma estatal.

II. LOS ESTÁNDARES DE PROTECCIÓN DE DATOS PERSONALES PARA LOS ESTADOS IBEROAMERICANOS

De forma previa al acercamiento a los Estándares que constituyen el sustrato de este apartado, hemos de detenernos en mencionar la contextualización internacional que hace la doctrina cuando habla del *constitucionalismo digital* como una tendencia teórica del derecho constitucional actual en virtud de la cuál se ha de garantizar la protección mediante normas comunes de reconocimiento y afirmación de derechos fundamentales en la era digital, proveyendo de especial tratamiento al dato personal como activo esencial para las empresas y agentes de comercio[2].

La aparición y desarrollo de las tecnologías de la información y de la comunicación a nivel universal han llevado a una manera distinta de comprender los derechos humanos puesto que la tecnología informática aporta una significación diferente a una serie de principios éticos que precisan de un modelo jurídico distinto. Motivo por el que, como se ha expuesto, el derecho constitucional debe recoger nuevas categorías de derechos humanos[3].

Partiendo de la generalidad de los principios mínimos que deben recogerse a nivel constitucional en las distintas normativas, para estudiar lo establecido

[2] LINDEN RUARO, R., y PIÑEIRO RODRIGUEZ, D., "La influencia europea sobre las leyes de protección de datos personales en latinoamérica: algunas reflexiones a partir de la perspectiva brasileña y en la base del constitucionalismo digital", en PIÑAR MAÑAS, J.L. (dir.), *Privacidad en un mundo global*, Valencia 2023, pp. 159-180, p. 173.

[3] AMOROSO, Y., y GUERRERO, J. "El panorama legislativo de la protección de datos en Latinoamérica en el período 2018-2022", en *Desafíos Jurídicos La Conjugación del Derecho*, 3 / 4 (2023) 50-77, p. 56.

en cada uno de los estados que se han ocupado en regular la materia, se ha de tener en cuenta, por un lado, que existen elementos comunes basados en el Reglamento europeo, pero, por otro lado, que existen también diferencias de categorías más específicas[4].

En los países latinoamericanos, si bien los legisladores se han basado en el sistema europeo en lo que al reconocimiento y protección del derecho se refiere, la evolución de cada regulación por países no ha sido simétrica, sino que existen en la actualidad países con niveles de protección adecuados y otros que tan sólo disponen de una protección mínima. Esto dibuja un marco complejo puesto que, con motivo de las importantes relaciones comerciales que muchos países de Latinoamérica tienen con Europa, precisan de una armonización normativa al Reglamento europeo, sin embargo, cada legislador ha introducido en su normativa en la materia particularidades distintas que hacen muy difícil en muchos países alcanzar niveles de seguridad que cumplan con los elevados requerimientos que marcó el regulador europeo[5].

En este contexto global, para realizar una aproximación a la regulación de estos países hemos de indicar que existen, según lo expuesto por la doctrina[6], unos estándares iberoamericanos que recogen principios que orientan a los Estados de Iberoamérica en las reformas de sus legislaciones para que se lleven a cabo de forma homogénea en la región y que, unido al cuerpo de Principios sobre la Privacidad y la Protección de Datos Personales creado por el Comité Jurídico Interamericano de la Organización de los Estados Americanos, constituyen un instrumento informador fundamental de la legislación de los estados latinoamericanos y un enlace entre el RGPD y los Estados de América Latina.

Fue en el XV Encuentro Iberoamericano de Protección de Datos, cuando la Red Iberoamericana de Protección de Datos (en adelante RIPD o Red) aprobó oficialmente los llamados "Estándares de Protección de Datos de los Estados Iberoamericanos". Con ello se pretendía dar cumplimiento al objetivo de los miembros de la Red consistente en la formulación de unos principios que sirvieran de eje vertebrador de los procesos legislativos que debían llevarse a cabo en el marco de cooperación entre los Estados en materia de privacidad y protección de datos.

[4] *Ibidem*, p. 57.

[5] *Ibidem,* p. 76.

[6] ALBORNOZ, M. M., "Expansión del ámbito territorial de aplicación de la ley en materia de protección de datos personales: ¿Tendencia en América Latina?", en *Latin American Law Review,* nº 09 (2022) 139-160, p. 146. https://doi.org/10.29263/lar09.2022.08.

El primer aspecto que se establece reside en que el ámbito de aplicación de los estándares será el tratamiento de los datos personales realizado por un responsable o encargado establecido en territorio de los Estados Iberoamericanos, inspirado claramente en el artículo 3.1. del RGPD. Este criterio del establecimiento como vínculo con el territorio es un aspecto común entre el RGPD y los Estándares, sin embargo, también se aprecian diferencias como que en los Estándares no se exige que se lleve a cabo el tratamiento en actividades del establecimiento y se admite que puede haber varios establecimientos[7].

Existe igualmente el criterio del *targeting* en el artículo 5.1.b. de los Estándares replicando lo establecido en el artículo 3.2 del RGPD, es decir, cuando las actividades del tratamiento estén dirigidas a los destinatarios de bienes y servicios residentes en los estados iberoamericanos, serán de aplicación los citados Estándares. Encontramos aquí otra diferencia importante respecto del RGPD puesto que en nuestro Reglamento sólo se exige que se encuentren en Estados de la Unión Europea.

El artículo 5.1.c. establece que quedarán sometidos a los Estándares aquellos responsables que se encuentren bajo el ámbito de aplicación del derecho de alguno de los Estados iberoamericanos en virtud del derecho internacional público o por la celebración de un contrato, criterio que sí se cumple en el RGPD en relación con aquellos responsables que no estén establecidos en un Estado miembro, pero queden sometidos en virtud del Derecho Internacional Público, no resulta así sin embargo en el RGPD para los que otorguen un contrato.

A lo largo de los Estándares encontramos otras importantes similitudes con elementos clave establecidos en el RGPD como son las siguientes[8]:

La obligación de realizar notificaciones de vulneraciones a la seguridad de los datos personales en el artículo 22 de los estándares que a su vez se refleja en el RGPD en el artículo 33.

El principio de responsabilidad proactiva en el considerando 23 y en el Capítulo VI de los estándares que es fiel reflejo del artículo 5.2. del RGPD.

Se recoge en el artículo 41 de los estándares la obligación de realizar una evaluación de impacto cuando el responsable detecte un elevado riesgo de

[7] *Ibidem,* p. 147.

[8] Estándares de Protección de Datos de los Estados Iberoamericanos, 20 de junio de 2017. [En línea]. Fecha de consulta: 31 de marzo de 2025. Disponible en: https://www.redipd.org/documentos/estandares-iberoamericanos-2017.

afectación al derecho a la protección de los datos personales; de igual forma que se establece en el artículo 35 del RGPD. No obstante, en los estándares se deja a elección del legislador de cada Estado, la fijación de los supuestos en los que será necesaria la evaluación de impacto.

La autoridad de control está regulada en el RGPD en el artículo 51 al 67 y se establece la misma obligación que se indica en el artículo 42 de los estándares, es decir, en cada Estado miembro deberá existir una entidad de control independiente que asegure el cumplimiento de la normativa en la materia.

Otro elemento que vertebra los estándares es la protección de la intimidad y la circulación transfronteriza de datos personales que facilite el flujo entre los Estados iberoamericanos y a otras zonas del mundo, de igual forma que se recoge en el artículo 20 del RGPD cuando regula la portabilidad de los datos concediendo el derecho al titular de los datos de transmitirlo a otro responsable cuando sea técnicamente posible.

En el artículo 49 de los estándares y bajo la denominación de oficial de protección de datos personales, se regula la figura del Delegado de Protección de Datos Personales "europeo" recogido en los artículos 37 y siguientes del RGPD, las situaciones en las que resulta preceptiva su designación, así como sus funciones. Todo ello tomando en consideración que, tanto en los estados iberoamericanos como en la Unión Europea, el legislador de cada Estado podrá profundizar en cuestiones como los requisitos para su selección, el tipo de vinculación -laboral o mercantil- que tenga con la organización, así como otras funciones dentro de la entidad responsable con las que puede ser compatible la posición.

Respecto de las infracciones y sanciones, los estándares dejan en manos de los legisladores nacionales de los estados iberoamericanos el establecimiento de las medidas correctivas y del régimen sancionador frente a conductas que vulneren la legislación aplicable. Por su parte, en el considerando 129 del RGPD se recogen los plenos poderes de investigación, sanción, correctivos, autorización y consultivos que cada Estado ostentará a través de las autoridades de control para garantizar el cumplimiento de la normativa aplicable en la materia.

El considerando 135 del RGPD fija también el deber de establecer mecanismos que aseguren la cooperación entre los Estados miembros cuando las violaciones del marco regulatorio en asuntos de protección de datos afecten a varios Estados de la Unión. Este elemento se describe como objetivo fundamental de los estándares ya que se pretende favorecer la cooperación internacional entre

las autoridades de control de los Estados iberoamericanos y con las autoridades de control de fuera de la región[9].

En resumen y aunque con las diferencias expuestas entre los estándares y el RGPD, así como con otras que requieren de un estudio más pormenorizado de ambos textos, podemos indicar que dicho documento resulta una fuente informadora fundamental para los legisladores de los Estados iberoamericanos en materia de protección de datos de carácter personal.

La doctrina es clara en este sentido cuando asegura que al menos veinte países latinoamericanos basan su regulación en protección de datos de carácter personal en el sistema europeo con los mismos principios generales del tratamiento, derechos de los titulares, obligaciones para controladores y operadores de datos…[10].

El motivo principal que ha llevado a esos países a tomar en consideración el modelo europeo reside en que establece unos principios y derechos comunes que todos los Estados pueden seguir; asegura el efectivo ejercicio del derecho de protección de datos personales y favorece la portabilidad transfronteriza de los datos y la cooperación internacional entre las autoridades de control; todo ello para adecuarse al contenido mínimo en la materia aceptado internacionalmente y que tiene en el RGPD su referente más importante.

III. ANÁLISIS COMPARATIVO DEL RGPD Y LA LOPDGDD CON LA NORMATIVA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL DE LOS PAÍSES LATINOAMERICANOS

3.1. *Uruguay*

La figura del DPD en el Derecho de Uruguay sigue las líneas marcadas por parte del RGPD europeo. Uruguay cuenta con la Ley Nº 18.331, de 11 de agosto de 2008, que ha sido desarrollada reglamentariamente por el Decreto N° 414/2009 de 31 de agosto de 2009, Decreto que fijó los criterios que marcan el ámbito de aplicación de la ley: por un lado, que el tratamiento sea llevado a cabo por un responsable que realice la actividad o que esté establecido en Uruguay y por otro, que, sin estar establecido en Uruguay, use para el tratamiento de datos medios utilizados en el país.

Posteriormente, a través del artículo 37 de la Ley Nº 19.670, de 15 de octubre de 2018, para adecuar la norma al RGPD, se añaden dos nuevos supuestos en

[9] *Ibidem,* p. 4.

[10] LINDEN RUARO, R., y PIÑEIRO RODRIGUEZ, D. "La influencia europea sobre las leyes…", o. c., p. 162.

el ámbito de aplicación subjetivo de la ley cuando el responsable no está establecido en Uruguay como son: que las actividades de tratamiento estén dirigidas a habitantes uruguayos bien por la oferta de bienes o servicios o bien por analizar su comportamiento; o que lo establezca un contrato o el derecho internacional público. Todo ello, a tenor de lo considerado por la doctrina, ha redundado en una evolución positiva de los supuestos contemplados por el legislador de este país adaptados al RGPD[11]. Los artículos 10 a 15 del Decreto Nº 64/2020, de 21 de febrero de 2020, los Decretos Nº 664/008 de 22 de diciembre de 2008 y las resoluciones Nº 32 y Nº 44/2020 completan la reglamentación de esta materia en Uruguay.

En este ordenamiento jurídico el DPD se erige como un garante fundamental de la responsabilidad proactiva y de la responsabilidad de las entidades en materia de protección de datos, tal y como indica la doctrina más autorizada[12].

En cuanto a las entidades obligadas a disponer del DPD, una vez transcurren noventa días desde el inicio del procesamiento de datos, tienen ya la obligación de designarlo. Así mismo, tienen esa obligación en los siguientes casos: entidades públicas estatales y no estatales; entidades total o parcialmente de propiedad estatal; entes privados que tienen como actividad principal el procesamiento de datos y compañías que procesan datos de más de 35.000 personas.

Encontramos una similitud parcial con nuestro derecho respecto del tema estudiado a lo largo de este trabajo ya que obliga a las entidades públicas, así como a las entidades privadas con participación pública, a disponer de esta figura, podríamos entender aquí incluidas las sociedades mercantiles compuestas por capital público. En nuestro derecho, el artículo 37.1 del RGPD establece los casos en los que es obligatoria la designación del DPD entendiendo cuando el tratamiento es llevado a cabo por una autoridad u organismo público; cuando las actividades principales de la entidad responsable son el tratamiento de datos y cuando su actividad consiste en el tratamiento de datos a gran escala.

Se aprecia otra similitud con nuestro derecho en la posibilidad que existe en Uruguay de poder nombrar un único DPD para varias entidades que conforman una única unidad estructural administrativa, con la particularidad de que la autoridad en materia de protección de datos en Uruguay (Unidad Reguladora y de control de datos Personales) puede trasladar un requerimiento para que se nombre un DPD adicional dentro de esa estructura. En nuestro derecho en

[11] *Ibidem,* p. 155.

[12] BRIAN NOUGRERES, A., "Uruguay: El Delegado de Protección de Datos en Uruguay", en *La Ley privacidad*, nº. 9 (2021) 1.

virtud de lo establecido en el artículo 37.3. del RGPD se puede designar un único DPD para varias entidades.

Otra cuestión similar del régimen de contratación del DPD en Uruguay con respecto al derecho español reside en la posibilidad de que el DPD esté bajo una relación laboral o bajo una externalización de servicios a través de un contrato mercantil, aspecto establecido en el 37.6 del RGPD.

Idéntica a las previsiones establecidas en nuestro derecho, resulta la necesidad de independencia del DPD en el sentido de no incurrir en conflictos de intereses y de su autonomía técnica, es decir, imposibilidad de recibir instrucciones del responsable. De igual forma que en la normativa uruguaya es el responsable del tratamiento de los datos el que designa el DPD, se indica también así en el artículo 37 del RGPD[13].

Si bien existe una clara semejanza entre la norma uruguaya de protección de datos y el derecho aplicable en nuestro país respecto de la necesidad de formación jurídica que ha de tener el DPD, formación en herramientas informáticas y en seguridad de la información así como la experiencia previa en el campo de la protección de datos; encontramos elementos adicionales que añade la autoridad de control en esta materia en Uruguay y que no se dan en nuestro derecho: recomienda el conocimiento del área de negocio y habilidades de comunicación y de negociación[14].

Las funciones del DPD son las mismas en uno y otro ordenamiento jurídico: supervisar el cumplimiento de la normativa aplicable en la materia, diseño y puesta en marcha de políticas de protección de datos, colaboración con la autoridad de control, introducción de medidas para la adaptación de la empresa a la normativa nacional e internacional y asesorar en la materia en todas las situaciones que impliquen un riesgo para la privacidad de los datos o un tratamiento de datos personales.

Debido a que el DPD es un asesor y consultor, el desempeño de sus funciones no implica obligatoriedad de cumplimiento normativo por su parte sino por parte del responsable del tratamiento al que asesora, por lo que no puede derivarse de la realización de sus funciones, como tampoco sucede en nuestro derecho, responsabilidad de tipo penal ni administrativa[15].

[13] *Ibidem,* p. 2.
[14] *Ibidem,* p. 3.
[15] *Ibidem,* p. 4.

3.2. *Perú*

La norma vigente hasta marzo de 2025 guardaba enormes similitudes con la norma mexicana que regula esta materia por la influencia que tuvo en el legislador peruano lo establecido en el ordenamiento jurídico mexicano[16]. Sin embargo, en el ordenamiento jurídico peruano cuentan con una reciente norma publicada el 30 de noviembre de 2024, el Decreto Supremo N° 016-2024-JUS que aprueba el Reglamento de la Ley N° 29733, Ley de Protección de Datos Personales, derogando el anterior a partir del 30 de marzo de 2025. Algunos de los principales cambios que opera esta ley son[17]:

La inclusión de las actividades que incluyen manejo de datos personales para la comercialización de bienes y servicios y las relacionadas con el análisis del comportamiento del consumidor, que suponen una importante novedad respecto de la anterior legislación peruana en la materia[18].

Se introduce también la designación de un representante del tratamiento en el país que sea el punto de contacto con la autoridad nacional de protección de datos, aspecto similar al que se regula en el artículo 36 de nuestra LOPDyGDD ya que es el DPD el interlocutor de la entidad responsable con la AEPD. Esta figura, se denomina en Perú Oficial de Cumplimiento de Datos Personales y debe ser designado por el responsable de los datos cuando se haga un tratamiento de macrodatos personales, o cuando afecten a un gran número de personas, se traten datos sensibles, o cuando se cause un perjuicio evidente a los derechos o libertades del titular del dato personal; similar a lo previsto en el artículo 37.1 del RGPD. Se puede designar un solo Oficial de Cumplimiento de Datos Personales para un grupo empresarial, coincidente con lo previsto también en el artículo 37.2 del RGPD.

Si bien existen estas dos últimas similitudes en lo relativo a la designación del DPD entre la legislación europea y peruana, el Reglamento europeo recoge también la posibilidad de designar un único DPD para varias administraciones públicas considerando su estructura y tamaño según se prevé en el artículo 37.3.

---

[16] ALBORNOZ, M. M., "Expansión del ámbito territorial de aplicación de la ley en materia de protección de datos personales: ¿Tendencia en América Latina?", o. c., p. 153.

[17] TOVAR, T., "Nuevo reglamento de la Ley de Protección de Datos Personales", 3 de diciembre de 2024. [En línea]. Fecha de consulta: 19 de marzo de 2025.

Disponible en: https://www.echecopar.com.pe/publicaciones-nuevo-reglamento-de-la-ley-de-proteccion-de-datos-personales.html.

[18] MUSCHI, F., "Perú: Se publica el nuevo Reglamento de la Ley de Protección de Datos Personales", 3 de diciembre de 2024. [En línea]. Fecha de consulta: 21 de marzo de 2025. Disponible en: https://www.garrigues.com/es_ES/noticia/peru-publica-nuevo-reglamento-ley-proteccion-datos-personales.

Como último aspecto destacable de la nueva reglamentación peruana respecto del Oficial de Cumplimiento de Datos Personales, resulta necesario indicar, que, de igual forma que está estipulado en nuestro derecho en el artículo 35 de la LOPDGDD, debe acreditar una formación especializada y práctica en protección de datos. Puede así mismo desempeñar otras funciones en el seno de la organización o ser externo tal y como está previsto también en el artículo 37.6 del RGPD[19].

Realizada la breve comparativa de la figura del DPD en Perú con la configuración que tiene en nuestro derecho, abordamos ahora otras diferencias y coincidencias relevantes en la materia de protección de datos en general entre las regulaciones de uno y otro Estado.

Al igual que existe en nuestra LOPDGDD en el artículo 11.2, en la nueva norma peruana se prevé que el titular de los datos debe recibir información adicional si sus datos van a utilizarse para la elaboración de perfiles y se debe indicar la fuente desde donde se obtienen los datos si no proceden directamente del titular, tal y como figura en el artículo 11.3 de nuestra norma.

El legislador peruano ha incluido la obligación que recae en el responsable de los datos consistente en hacer todos los esfuerzos razonables por acreditar la identidad de quienes otorgan el consentimiento de un menor de edad, de igual forma que prevé el artículo 8.2 del RGPD. El incumplimiento de esta obligación está previsto también en nuestra norma en el artículo 73 como infracción grave, con clara similitud a lo previsto en la norma peruana.

La norma peruana prevé la recopilación de datos con fines publicitarios, como así se recoge también en el RGPD siempre que se informe de todos los aspectos previstos en los artículos 13 y 14 así como "en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo", según exige el artículo 12 RGPD.

Se deben notificar y documentar los incidentes de seguridad, entendiendo como tales las posibles vulneraciones, pérdidas o alteración ilícita de los datos, cuestión abordada también por el legislador europeo en el considerando 49 y en el artículo 33 del RGPD.

[19] GÁLVEZ, A., "Nuevo reglamento refuerza la protección de datos personales", en *Revista digital de la Cámara de Comercio de Lima,* 16 de diciembre de 2024. [En línea]. Fecha de consulta: 20 de marzo de 2025. Disponible en:
https://lacamara.pe/nuevo-reglamento-refuerza-la-proteccion-de-datos-personales/.

Otra cuestión importante en la que se encuentran grandes similitudes entre el RGPD y la nueva norma peruana reside en las medidas de seguridad respecto de los datos que debe adoptar el responsable. En el artículo 32 del RGPD se fija la obligación de adoptar las medidas técnicas y organizativas que debe adoptar el responsable del tratamiento para garantizar la seguridad en función de los riesgos y del sistema utilizado para el tratamiento, entre ellas la elaboración de un inventario de activos partiendo de la descripción sistemática del tratamiento. En la norma peruana se establecen dos obligaciones nuevas: generación de un inventario de los datos personales y de los sistemas empleados para el tratamiento y realizar copias de seguridad de periodicidad semanal.

Otro aspecto que introduce la nueva norma peruana y que se toma del RGPD es el derecho del titular de los datos a la portabilidad de los mismos de un responsable a otro cuando sea técnicamente posible, tal y como establece el artículo 20 del RGPD y en el derecho español por la remisión del artículo 17 de la LOPDGDD.

La nueva norma peruana incluye como atenuantes de una posible sanción administrativa la implementación de códigos de conducta y de evaluaciones de impacto del tratamiento de datos realizado[20], asunto que se encuentra recogido parcialmente en el Artículo 83.2.k) del RGPD cuando considera como atenuante de una posible sanción administrativa para el responsable, la adhesión a códigos de conducta. En relación con los procedimientos sancionadores, en la nueva norma peruana se concretan mejor las infracciones y sanciones derivadas de incumplimientos de la normativa y queda regulado expresamente el caso de reincidencia[21].

Se establece en la norma peruana la obligación de contar con un documento de seguridad en el que se incluyan la gestión de accesos a los datos, las verificaciones periódicas asignadas a determinados sistemas, el tratamiento de datos para la publicidad…, en general, las medidas y procedimientos de seguridad implementadas por la entidad. En igual sentido que se ha dado en España con los documentos aprobados y actualizados para dar cumplimiento a las premisas de responsabilidad proactiva y control de riesgos proclamadas por el RGDP[22].

En relación con la normativa anterior peruana y como aspecto novedoso de la nueva regulación, en el caso de transferencia de datos a otros estados,

[20] TOVAR, T., "Nuevo reglamento de la Ley de Protección de Datos Personales", o. c.

[21] MUSCHI, F. "Perú: Se publica el nuevo Reglamento de la Ley de Protección de Datos Personales", o. c.,

[22] GÁLVEZ, A., "Nuevo reglamento refuerza la protección de datos personales", o. c.

se podrán realizar siempre y cuando el estado de destino de los datos tenga un marco jurídico y unos principios de protección de los datos, normativa garantista de los derechos de los titulares de los datos y su ejercicio, así como la existencia de una entidad supervisora del cumplimiento de la normativa[23].

En resumen, según la doctrina[24] la nueva norma adoptada en Perú supone un enorme paso en la evolución de la protección de datos en Perú debido a la adaptación a las nuevas tecnologías que supone en esta materia y en el establecimiento de normativa pormenorizada que refleja con claridad las obligaciones de las empresas en protección de datos de carácter personal.

3.3. *México*

México requiere también una mirada obligada en este breve análisis comparativo con nuestro derecho puesto que cuenta desde el 20 de marzo de 2025 con una nueva ley en esta materia que cambia la configuración del Oficial de Datos Personales y su designación.

Si analizamos someramente la nueva Ley General de Protección de Datos Personales en posesión de sujetos obligados publicada en el Diario Oficial de la Federación el 20 de marzo de 2025, encontramos cómo a partir de ahora el Oficial de Datos Personales será nombrado por el ejecutivo federal a través del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (en adelante INAI).

Se recoge una definición de la figura similar a la que podemos deducir en Europa ya que según el informe "Recomendaciones para los sujetos obligados en la designación del oficial de protección de datos personales" creado por el INAI, el oficial de protección de datos personales se define como la persona especialista en la materia quien auxilia y orienta al titular que lo requiera con relación al ejercicio del derecho de protección de datos personales y en sede interna del sujeto obligado se encarga de asesorar a las áreas y de realizar las gestiones necesarias para el manejo, mantenimiento, seguridad y protección de los sistemas de datos personales[25].

[23] MUSCHI, F., "Perú: Se publica el nuevo Reglamento de la Ley de Protección de Datos Personales", o. c.

[24] MEJÍA, B., "Protección de Datos Personales en Perú: nuevo reglamento y su impacto en las empresas peruanas", 28 de enero de 2025. [En línea]. Fecha de consulta: 20 de marzo de 2025. Disponible en: https://www.ey.com/es_pe/insights/law/proteccion-datos-personales-peru-nuevo-reglamento.

[25] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. México., en "Recomendaciones para los sujetos obligados en la designación del oficial de protección de datos personales", p. 9.

Como también se encuentra en nuestro derecho, pero con la diferencia de que no se fijan unos supuestos claros de obligatoriedad de designación, la designación del Oficial de Datos Personales no es obligatoria en la nueva ley. El artículo 79 de la misma establece que cada responsable deberá tener una Unidad de Transparencia que se ajustará a lo establecido en la Ley General de Transparencia y Acceso a la Información Pública y que cuando se lleven a cabo tratamientos de datos relevantes o intensivos, podrán solicitar la designación de un oficial de protección de datos personales especializado en la materia.

En cuanto al proceso de designación, no se requiere ningún protocolo específico, pero se recomienda que se sigan los procedimientos internos que tenga la organización en este sentido[26].

Las principales funciones que tendrá atribuidas serán: fomento de la cultura de protección de datos, identificar mejores prácticas, asesorar a las áreas de la entidad en esta materia, atención de quejas y reclamaciones, evaluar las prácticas de protección de datos en la organización, proponer al comité de transparencia políticas, programas y acciones para cumplir con la legalidad…, con clara similitud a lo establecido en el RGPD.

Para las entidades públicas, será la Unidad de Transparencia la que pueda fijar un Oficial de Datos Personales cuando se realicen tratamientos de datos personales relevantes o intensivos[27]. No hay una descripción clara de las entidades públicas obligadas y las que no, simplemente la facultad de la Unidad de Transparencia de designarlo en determinados casos, a diferencia de lo recogido al respecto en nuestro derecho.

Estudiando otras cuestiones generales de la nueva ley que pueden asemejarse a lo dispuesto en nuestra normativa de aplicación en materia de protección de datos, el responsable de los datos, según el artículo 29 de la citada ley, deberá establecer, de igual forma que sucede en nuestro ordenamiento jurídico, un documento de seguridad en el que se incluyan los datos personales, el sistema de tratamiento, los posibles riesgos, las posibles brechas, el plan de trabajo sobre la materia…

Una nueva entidad reemplaza a la citada INAI, se trata de la Secretaría de Anticorrupción y Buen Gobierno, que será a partir de la entrada en vigor de

[26] PADILLA ESPINOSA, M., "El Oficial de Protección de Datos Personales en México", 25 de marzo de 2025. [En línea]. Fecha de consulta: 29 de marzo de 2025. Disponible en: https://todopdp.com/el-oficial-de-proteccion-de-datos-personales-en-mexico/

[27] *Ibidem.*

la nueva ley la autoridad en materia de protección de datos personales para particulares[28].

Se permite que los responsables establezcan medidas de autorregulación internas que permitan cumplir la nueva normativa y adaptar sus políticas internas en esta materia, cuestión muy similar a la facultad del responsable de establecer las políticas en la materia internamente en la organización, recogida en nuestro ordenamiento jurídico.

Otra cuestión remarcable es que se regulan en el artículo 60 las transferencias de datos internacionales siempre que estén reguladas por ley o tratado internacional ratificado por México y con las finalidades compatibles con las que originaron el tratamiento.

En materia de infracciones y sanciones se establece la Unidad de Medida y Actualización para las sanciones, sustituyendo el salario mínimo como criterio de medición. Se incluye también la negligencia y el dolo como elemento que sustente las posibles infracciones del ejercicio de los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición)[29].

3.4. *Chile*

Asistimos también en el caso del ordenamiento jurídico chileno a una reciente aprobación de la norma reguladora de protección de datos, tal y como sucede en Perú y México de igual forma, basada en gran parte en el RGPD de la Unión Europea.

La ley 21719 publicada el 13 de diciembre de 2024 regula la protección y el tratamiento de los datos personales, crea la agencia de protección de datos personales y concede a las entidades chilenas responsables de datos un periodo de adaptación para su adecuado cumplimiento de veinticuatro meses desde su publicación.

En el ámbito territorial de aplicación de la ley, resulta remarcable la similitud con el derecho español en cuanto a que se aplicará a quienes realicen tratamiento

[28] SERRANO, J. L. *et al*., "México: La nueva Ley Federal de Protección de Datos Personales en Posesión de los Particulares introduce conceptos como el aviso de privacidad y elimina el INAI", 27 de marzo de 2025 [En línea]. Fecha de consulta: 29 de marzo de 2025. Disponible en: https://www.garrigues.com/es_ES/noticia/mexico-nueva-ley-federal-proteccion-datos-personales-posesion-particulares-introduce.

[29] *Ibidem*.

de datos en territorio nacional, a quienes lo realicen en representación de un mandatario que se encuentre en territorio nacional y cuando el tratamiento esté destinado a la prestación de bienes y servicios en el país.

Para el cumplimiento y fiscalización de la normativa de protección de datos, se crea la Agencia de Protección de Datos[30], ente ya existente en España desde 1992, así como en otros países de Latinoamérica en los que se ha procedido a actualizar la normativa en esta materia recientemente con otra denominación.

De manera similar a lo previsto en el Reglamento europeo y en nuestra norma estatal, se establece en la nueva norma chilena un régimen severo de infracciones y sanciones a fin de preservar y garantizar la seguridad de los datos. Se penaliza la reiteración de infracciones, de forma similar a lo establecido en el artículo 83.2.e) RGPD y en el 76.2.a) de la LOPDGDD, preceptos que recogen el carácter continuado de la infracción.

Con el fin de mantener un control e información pública sobre las entidades sancionadas por incumplimiento de la normativa, se crea el Registro Nacional de Sanciones y Cumplimiento[31] similar al Registro de las actividades del tratamiento previsto en los apartados 1 y 2 del artículo 30 del RGPD y en el 31.1 de la LOPDGDD aunque no se incluyan en el Registro español las sanciones y sea obligatorio sólo para entidades en los casos especificados en el apartado 5 del artículo 30 citado.

Según el propio gobierno chileno, el objetivo del legislador es implementar una norma basada en un referente internacional en esta materia como es el RGPD europeo y lograr así alcanzar el adecuado nivel de protección de datos exigido por la Comisión Europea a efectos de garantizar una segura transferencia internacional de los datos en las operaciones comerciales de la Unión Europea con Chile, así como cumplir con los compromisos adquiridos por este país con la OCDE en 2010[32].

El legislador chileno regula también el derecho de portabilidad de los datos para que el titular de los datos tenga derecho a obtener una copia en un

[30] GOBIERNO DE CHILE, "Se aprueba Ley de Protección de Datos Personales: Revisa de qué se trata", 27 de agosto de 2024. [En línea]. Fecha de consulta: 23 de marzo de 2025. Disponible en: https://www.gob.cl/noticias/ley-proteccion-datos-personales-aprobacion-eleva-estandar-derechos/.

[31] HASSI, S. "Chile: Aprobada la Ley de Protección de Datos Personales", 9 de septiembre de 2024. [En línea]. Fecha de consulta: 23 de marzo de 2025. Disponible en: https://www.garrigues.com/es_ES/noticia/chile-aprobada-ley-proteccion-datos-personales.

[32] GOBIERNO DE CHILE. "Se aprueba Ley de Protección de Datos Personales: Revisa de qué se trata", o. c.

formato operativo a través de distintos sistemas y puedan transferirse si le interesa a otros responsables; siguiendo el criterio establecido también en el artículo 20 del RGPD aplicable en España según la remisión del artículo 17 de la LOPDGDD.

El tratamiento de los datos por parte del responsable queda legitimado no sólo por el consentimiento del titular sino también con motivo del cumplimiento de obligaciones legales, de la ejecución de contratos y del interés legítimo del responsable.

Tal y como se realiza en nuestro país (artículo 28 de la LOPDGDD) y proclama el RGPD en el artículo 35, se establece en la norma chilena la obligación para el responsable de los datos consistente en llevar a cabo una evaluación de impacto en los casos en los que se realice tratamiento de macrodatos y existan elevados riesgos de vulneración de los derechos de los titulares. En tal caso se consultará a la Agencia Estatal de Protección de datos para recibir recomendaciones sobre cómo actuar[33].

3.5. *Ecuador*

En Ecuador ya el 26 de mayo de 2021 publicaron la Ley Orgánica de Protección de Datos Personales que ha sido desarrollada reglamentariamente por el Reglamento de la Ley Orgánica de Protección de Datos Personales, norma número 904 publicada el 13 de noviembre de 2023 en el Registro Oficial Suplemento.

La aplicación subjetiva de dicha Ley recoge cuatro supuestos: aquellas entidades que realicen el tratamiento en territorio ecuatoriano, las que tengan el domicilio del responsable en Ecuador, cuando el *targeting* sea hecho por un responsable que resida en Ecuador o que no resida pero preste servicios o produzca bienes o realice funciones de control de comportamiento en Ecuador y por último, será de aplicación por motivo de la vinculación a través de la regulación contenida en el derecho internacional público o a través de un contrato aunque no esté establecido en Ecuador.

Los primeros criterios de aplicación se basan en los establecidos en el artículo 3.1. del RGPD sin embargo, tal y como indica la doctrina, se aprecia que el legislador ecuatoriano ha pretendido mantener el criterio de la territorialidad introduciendo el *targeting* aunque el responsable no esté domiciliado en Ecuador, cuestión que no se recoge en el RGPD[34].

[33] HASSI, S., "Chile: Aprobada la Ley de Protección de Datos Personales", o. c.

[34] ALBORNOZ, M. M., "Expansión del ámbito territorial de aplicación de la ley en materia de protección de datos personales: ¿Tendencia en América Latina?", o. c., p. 153.

La doctrina en Ecuador ha dejado clara la influencia del RGPD en la LOPD de Ecuador como así se refleja en el nuevo modelo que se infiere de dicha norma, con estándares internacionales similares a los aplicados en la Unión Europea, que abarcan desde la gestión de los datos hasta un uso más adecuado de los mismos que se ve reflejado en la garantía de los principales derechos de los usuarios y en el rol más proactivo y con mayores obligaciones de los responsables[35].

Para ejemplificar someramente estas similitudes, se regulan aspectos ya tratados en este trabajo para otros ordenamientos jurídicos analizados como los siguientes:

La obtención de un consentimiento informado para recopilar la información y garantías de confidencialidad e integridad a través de auditorías y protocolos de seguridad. La designación de un DPD, como así se establece en el artículo 48 del reglamento de desarrollo, que aúne la preparación adecuada para el puesto, la independencia necesaria y la ausencia de conflictos de interés. De igual forma que sucede en nuestro derecho, puede ser contratado en régimen laboral o mercantil (artículo 49 de la Ley). Se crea la Autoridad de Protección de Datos Personales como entidad pública independiente encargada de la supervisión y cumplimiento de la normativa (artículo 4 de la Ley) y cuyas funciones se desarrollan en los artículos 75 y ss. Se establecen los principios inspiradores reconocidos internacionalmente en el artículo 10 de la Ley. El derecho a la portabilidad de los datos siempre que esté en un formato compatible se recoge en el artículo 17 de la Ley. La transferencia de datos con consentimiento del titular y cumpliendo las previsiones de la Ley. El establecimiento de medidas de seguridad en el sector público a tenor de lo expuesto en el artículo 38 de la Ley. La evaluación de impacto por los riesgos del tratamiento (artículo 42 de la Ley) y, por último, un régimen sancionador en los artículos 67 y ss.

En resumen, según ha tenido en cuenta la doctrina más autorizada en este país[36], Ecuador cuenta ya con una normativa básica y de desarrollo además de con una jurisprudencia en materia de protección de datos que permite su aplicación en las situaciones que se precise. Sin embargo, las empresas, la Administración Pública, así como los particulares aún adolecen de la concienciación necesaria en materia de privacidad para cumplir la normativa en esta materia y establecer los medios y medidas que garanticen la protección de los datos, a pesar de que la disposición transitoria primera de la Ley concedió dos años

[35] *Ibidem,* p. 89.

[36] ORDOÑEZ PINEDA, L., *et al.,* "Políticas públicas y protección de datos personales en Ecuador reflexiones desde la emergencia sanitaria.", en *Estado & comunes: Revista de políticas y problemas públicos*, 2 / 15, (Ejemplar dedicado a: Tecnologías en las políticas públicas sociales en América Latina), (2022) 77-97, p. 95.

para la adecuación de los responsables a los preceptos de esta y a su normativa de desarrollo.

3.6. *Argentina*

En Argentina la reforma de la Constitución operada en 1994 reconoce de forma oficial la protección de datos a nivel federal pero no se regula expresamente hasta la Ley de Protección de Datos Personales Nº 25.326 que regula el *Habeas Data* y el derecho de autodeterminación informativa, entrando en vigor una vez publicada en el Boletín Oficial de 2 de noviembre de 2000[37].

Es remarcable que Argentina fue pionero en la obtención de la declaración de la adecuación para la transferencia internacional de datos por la Comisión Europea. En el año 2003 la Comisión Europea mediante Decisión Nº 2003/490/EC resolvió que Argentina contaba con un nivel de protección de datos de carácter personal similar al de la Unión Europea y permitía que hubiera transferencia de datos sin ningún inconveniente ni condición.

La ley vigente en Argentina es la citada Ley Nº 25.326 publicada el 2 de noviembre de 2000 que regula el *Habeas Data* y configura el derecho de autodeterminación informativa. Esta norma ha sufrido dos reformas parciales, una mediante Ley Nº 26.343 sobre el blanqueo de deudores que habían caído en mora entre 2001 y 2003 y a través de la Ley Nº 26.388 de Delitos Informáticos que modificó el artículo 22 de sanciones penales[38].

En el desarrollo reglamentario posterior de la Ley se crea la autoridad de control en la materia: la Dirección Nacional de Protección de Datos Personales, que comenzó a tomar decisiones a través de resoluciones que ayudaron a interpretar la ley y los reglamentos. No obstante, fue un órgano sobre el que se puso en tela de juicio su independencia inicial. Este hecho motivó que, cuando se publicó la Ley de Acceso a la Información Pública Nº 27.275, se sustituyera por la Agencia de acceso a la Información Pública, que concedió mayor independencia al órgano supervisor en Argentina[39]; órgano similar al existente en nuestro país.

Con respecto al régimen jurídico en materia de protección de datos en este país, se han producido desde que está en vigor esta norma numerosos avances positivos:

---

[37] PERUZZOTTI, M. "Actualidad en materia de protección de datos personales en Argentina.", en *Cuaderno 217* | Centro de Estudios en Diseño y Comunicación (2024/2025) 191-203, pp. 192 y 193.

[38] *Ibidem.,* p. 193.

[39] *Ibidem,* p. 194.

En primer lugar, se creó el Registro Nacional de Bases de Datos tal y como existe en nuestro derecho el Registro de Actividades de tratamiento según lo establecido en el artículo 30 del RGDP y en el 31.1. de la LOPDyGDD.

Otro aspecto regulado por la norma argentina, ratificado por las resoluciones emitidas por la Agencia de Información Pública, ha sido la posibilidad del uso de la información personal para fines comerciales, tal y como recoge también el artículo 23 de nuestra Ley.

Otros elementos que se asemejan a nuestro derecho y a lo establecido en la Unión Europea son el régimen sancionador que establece el Capítulo VI de la norma argentina. Si bien existe una matización importante respecto de nuestro derecho ya que el legislador argentino incluye no sólo sanciones de tipo administrativo sino también penal, puesto que a través del artículo 32 de esta norma se incluye el artículo 117 bis del Código Penal argentino que recoge la posibilidad de sancionar con penas de prisión los casos de determinadas infracciones relacionadas con datos de carácter falso o conductas que vulneren las restricciones del banco de datos. Igualmente, para casos en los que se revele a otra entidad información del banco de datos o se vulneren sistemas de confidencialidad y seguridad, se incluye en la norma penal el artículo 157 bis, que recoge la facultad de imponer nuevamente sanciones privativas de libertad.

La norma argentina regula otros aspectos esenciales en la materia como son la obligación de seguridad y transferencia internacional de datos, recogidas también en nuestro ordenamiento jurídico, tal y como se ha expuesto.

Resulta importante mencionar que desde el poder legislativo se viene trabajando en un proyecto de actualización del régimen de protección de datos vigente desde el año 2022 tratando de seguir el estándar fijado en el RGPD. No ha tenido muchos avances desde entonces pero tal y como indica la doctrina, resulta necesaria una nueva regulación en la materia en Argentina que se adecue a la realidad actual. Esta actualización de la norma del 2000 ha sido considerada positivamente por la Comisión Europea a través de la última resolución que renovó la vigencia de la evaluación positiva obtenida por Argentina a un nivel de protección adecuado a efectos del artículo 45 del RGPD[40].

Atendiendo a la figura del DPD, diremos que es uno de los elementos que no se regula en la norma actual, sin embargo, en el proyecto de actualización si se incluye este rol y se hace con características muy similares a la concepción que se tiene en la Unión Europea y España. Este delegado será nombrado de forma

[40] *Ibidem,* p. 201.

obligatoria en unos casos y de manera voluntaria en otros; se describen en el proyecto los requisitos para poder ser Delgado, las tareas, el puesto…; se establece que para un grupo de empresas se podrá designar un único delegado de protección de datos y también que la posición se puede cubrir por un empleado interno o a través de un contrato externo de servicios[41].

Otro hito relevante en la regulación de los datos de carácter personal en Argentina es la adhesión al Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal Nº 108+ del Consejo de Europa a través de la Ley Nº 27.699[42]. Es en abril de 2023 cuando Argentina se convierte en el 23º Estado en ratificar el Convenio 108+ del Consejo de Europa, lo que posiciona a este país en el nivel de actor seguro en el mercado de datos adquiriendo el nivel más alto de protección de datos. Este documento consiste en una herramienta multilateral vinculante que tiene como finalidad la protección de la intimidad de los datos de las personas en el tratamiento de sus datos, lo que llevó a Argentina a una importante evolución en la protección de datos[43].

Igualmente, dentro del Plan Estratégico del 2022-2026 de la Agencia de Acceso a la Información Pública (AAIP), se asumió el compromiso de que las cláusulas de transferencias de datos internacionales se actualizasen tomando como referencia las Cláusulas Contractuales Modelo proporcionadas por la Red Iberoamericana de Protección de datos puesto que resultaban compatibles con la legislación argentina[44].

Cabe destacar también la aprobación por parte de la AAIP de un programa para la transparencia y protección de datos en la utilización de la Inteligencia Artificial que fue publicado en el Boletín Oficial mediante Resolución Nº 161/2023 de 4 de septiembre con el objetivo de impulsar las facultades del Estado en la protección de los datos en el sector público y privado garantizando el ejercicio de los derechos de los ciudadanos en la utilización de la inteligencia artificial[45].

Para finalizar este subapartado, podemos decir que si bien Argentina fue un estado pionero en disponer de una regulación en materia de protección de datos, coincidimos con la doctrina en la consideración de que se encuentra en pleno proceso de actualización y precisa incluir en su regulación elementos

[41] *Ibidem,* p. 198.
[42] *Ibidem,* p. 195.
[43] PERUZZOTTI, M., "Balance 2023: Protección de datos personales en Argentina.", en *LA LEY privacidad*, nº 18 (2023) 1-11, p. 5. Editorial La Ley.
[44] *Ibidem,* p. 8.
[45] *Ibidem,* p. 8.

clave como la responsabilidad proactiva, el delegado de protección de datos, obligaciones del responsable y el encargado, evaluación de impacto de la protección de datos, autoridad de control, régimen sancionador, transferencia transfronteriza de datos, menores, incidentes de seguridad…teniendo en cuenta que se ha comprometido a nivel internacional en el cumplimiento de la normativa de esta materia.

En todos los ordenamientos jurídicos estudiados encontramos cómo se ha dibujado un escenario de adecuación a los parámetros que más protección ofrece la regulación de protección de datos personales y se aprecia claramente el esfuerzo hecho por los legisladores a fin de armonizar su normativa a los estándares internacionales, pero sin llegar a concretarse las exigencias exactas para cada país[46].

Se ha considerado igualmente que la alineación de los órganos supervisores y de control estatales con una vocación transnacional ha contribuido a concienciar al legislador de cada estado de la urgencia de hacer compatibles las legislaciones nacionales con las normas internacionales en la materia[47].

IV. A MODO DE REFLEXIÓN FINAL

Una vez realizada una aproximación a lo establecido en relación con la protección de datos en las empresas en los principales ordenamientos jurídicos de Latinoamérica, procedemos a continuación a sugerir unos postulados a modo de reflexión final, que sirvan de base para futuros razonamientos jurídicos en el derecho proyectado en Latinoamérica en la materia estudiada.

En los ordenamientos jurídicos de varios países latinoamericanos (Perú, México, Chile) se han aprobado y publicado recientemente normas actualizadas y en países como Argentina y Uruguay se precisa de una actualización urgente de la normativa vigente en materia de protección de datos para dar cumplimiento a los compromisos internacionales adoptados en la materia. Todas estas normativas están basadas en los estándares iberoamericanos que sirven de puente entre dichas legislaciones y el RGPD.

Ante la oportunidad que el estado actual de la cuestión supone para los legisladores de estos países; se propone la posibilidad de que, en el desarrollo

[46] LINDEN RUARO, R., y PIÑEIRO RODRIGUEZ, D., "La influencia europea sobre las leyes…", o. c., pp. 177 y 178.

[47] *Ibidem,* p. 177.

reglamentario que se proyecte en los países con nueva normativa o en la actualización regulatoria que se realice en otros; se establezcan unos parámetros comunes que permitan la armonización jurídica en esta materia a las principales normativas internacionales, con el fin de que las relaciones comerciales existentes no se vean perjudicadas por la necesidad de seguridad jurídica en la nueva era empresarial en la que el dato personal se instituye como un activo esencial de la actividad comercial.

Entendemos, tal y como considera la doctrina estudiada, la necesidad de establecer unas recomendaciones comunes para la regulación en esta materia que favorezcan el tráfico comercial entre las empresas como son: ponderar adecuadamente los derechos de los usuarios y el flujo de información necesarios; dotar a los organismos de control y supervisión de medios que permitan el adecuado cumplimiento de la norma; definir de forma clara el órgano de control y su supervisor así como sus atribuciones y capacidad sancionadora; conceder un tiempo razonable a las empresas y al sector público para la implementación de los requerimientos que la normativa establezca; redactar con claridad los términos abordados por la ley sin generar conceptos jurídicos indeterminados y articular un régimen sancionador severo pero proporcional a las infracciones[48].

Coincidimos también con la doctrina en que toda esta regulación necesaria en materia de protección de datos que ha de recoger los contenidos mínimos expuestos, ha de converger asimismo, en unos elementos esenciales de carácter ético como son el respeto a la dignidad de la persona, la autodeterminación, la seguridad, la inclusión social, el consentimiento…, si bien la normación no puede vertebrar la protección del dato en el derecho a la privacidad puesto que existen conflictos de otra índole que se han de tener en cuenta. Además, se debe aplicar la norma en esta materia teniendo en cuenta el impacto de las tecnologías de la información disponibles en cada momento en los datos personales y en su protección.

Resulta evidente que los países de Latinoamérica que pretendan mantener o incrementar las relaciones comerciales entre empresas así como las colaboraciones de las instituciones públicas en cuestiones de ciberdelincuencia, acuerdos comerciales interestatales,…deben armonizar su regulación al Reglamento europeo como norma de referencia a nivel internacional, con el fin de contribuir al óptimo nivel de seguridad en la protección de los datos exigido entre empresas y administraciones públicas de los países estudiados así como de Latinoamérica con España y el resto de países europeos.

[48] MAYORGA-JÁCOME T., *et al*, "Historia de la normativa…", o. c., p. 18.

V. BIBLIOGRAFÍA

- ALBORNOZ, M. M., "Expansión del ámbito territorial de aplicación de la ley en materia de protección de datos personales: ¿Tendencia en América Latina?", en *Latin American Law Review,* nº 09 (2022) 139-160. https://doi.org/10.29263/lar09.2022.08.

- AMOROSO, Y., y GUERRERO, J., "El panorama legislativo de la protección de datos en Latinoamérica en el período 2018-2022", en *Desafíos Jurídicos La Conjugación del Derecho,* 3 / 4 (2023) 50-77.

- BRIAN NOUGRERES, A., "Uruguay: El Delegado de Protección de Datos en Uruguay", en *La Ley privacidad*, nº. 9 (2021).

- Estándares de Protección de Datos de los Estados Iberoamericanos 2017, 20 de junio de 2017. [En línea]. Fecha de consulta: 31 de marzo de 2025. Disponible en: https://www.redipd.org/documentos/estandares-iberoamericanos-2017.

- GÁLVEZ, A., "Nuevo reglamento refuerza la protección de datos personales." *Revista digital de la Cámara de Comercio de Lima,* 16 de diciembre de 2024. [En línea]. Fecha de consulta: 20 de marzo de 2025. Disponible en: https://lacamara.pe/nuevo-reglamento-refuerza-la-proteccion-de-datos-personales/.

- GOBIERNO DE CHILE, "Se aprueba Ley de Protección de Datos Personales: Revisa de qué se trata", 27 de agosto de 2024. [En línea]. Fecha de consulta: 23 de marzo de 2025. Disponible en: https://www.gob.cl/noticias/ley-proteccion-datos-personales-aprobacion-eleva-estandar-derechos/.

- HASSI, S., "Chile: Aprobada la Ley de Protección de Datos Personales", 9 de septiembre de 2024. [En línea]. Fecha de consulta: 23 de marzo de 2025. Disponible en: https://www.garrigues.com/es_ES/noticia/chile-aprobada-ley-proteccion-datos-personales.

- Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. México, "Recomendaciones para los sujetos obligados en la designación del oficial de protección de datos personales"

- Ley General de Protección de Datos Personales en posesión de sujetos obligados publicada en el Diario Oficial de la Federación el 20 de marzo de 2025. México.

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. *Boletín Oficial del Estado*, 6 de diciembre de 2018, nº 294.

- LINDEN RUARO, R., y PIÑEIRO RODRIGUEZ, D., "La influencia europea sobre las leyes de protección de datos personales en latinoamérica: algunas reflexiones a partir de la perspectiva brasileña y en la base del constitucionalismo digital", en PIÑAR MAÑAS, J.L. (dir.), *Privacidad en un mundo global*, (2023) 159-180.

- MAYORGA-JÁCOME T. C., *et al.,* "Historia de la normativa reguladora de la Protección de Datos de carácter personal en distintos países Latinoamericanos", en *Revista Científica Dominio de las Ciencias,* Vol. 5, nº 1 (enero 2019) 518-537.

- MEJÍA, B., "Protección de Datos Personales en Perú: nuevo reglamento y su impacto en las empresas peruanas" [En línea]. Fecha de consulta: 20 de marzo de 2025. Disponible en: https://www.ey.com/es_pe/insights/law/proteccion-datos-personales-peru-nuevo-reglamento.

- MUSCHI, F., "Perú: Se publica el nuevo Reglamento de la Ley de Protección de Datos Personales", 3 de diciembre de 2024. [En línea]. Fecha de consulta: 21 de marzo de 2025. Disponible en: https://www.garrigues.com/es_ES/noticia/peru-publica-nuevo-reglamento-ley-proteccion-datos-personales.

- ORDOÑEZ PINEDA, L., *et al.,* "Políticas públicas y protección de datos personales en Ecuador reflexiones desde la emergencia sanitaria", en *Estado & comunes: Revista de políticas y problemas públicos*, vol. 2, nº. 15 (2022) 77-97. Ejemplar dedicado a: Tecnologías en las políticas públicas sociales en América Latina.

- PADILLA ESPINOSA, M., "El Oficial de Protección de Datos Personales en México", 25 de marzo de 2025. [En línea]. Fecha de consulta: 29 de marzo de 2025. Disponible en: https://todopdp.com/el-oficial-de-proteccion-de-datos-personales-en-mexico/.

- PERUZZOTTI, M., "Actualidad en materia de protección de datos personales en Argentina" en *Cuaderno 217* | Centro de Estudios en Diseño y Comunicación (2024/2025) 191-203.

- PERUZZOTTI, M., "Balance 2023: Protección de datos personales en Argentina", en *LA LEY privacidad*, nº 18 (octubre de 2023) 1-11.

- Reglamento (UE) 2016/679 del parlamento europeo y del consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). *Diario Oficial de la Unión Europea.* 4.5.2016. I.119/ 1-I.119/88.

- SERRANO, J. L., *et al*., "México: La nueva Ley Federal de Protección de Datos Personales en Posesión de los Particulares introduce conceptos como el aviso de privacidad y elimina el INAI", 27 de marzo de 2025 [En línea]. Fecha de consulta: 29 de marzo de 2025. Disponible en: https://www.garrigues.com/es_ES/noticia/mexico-nueva-ley-federal-proteccion-datos-personales-posesion-particulares-introduce.

- TOVAR, T., "Nuevo reglamento de la Ley de Protección de Datos Personales", 3 de diciembre de 2024. [En línea]. Fecha de consulta: 19 de marzo de 2025. Disponible en: https://www.echecopar.com.pe/publicaciones-nuevo-reglamento-de-la-ley-de-proteccion-de-datos-personales.html.