Expansión del ámbito territorial de aplicación de la ley en materia de protección de datos personales: ¿Tendencia en América Latina?

María Mercedes Albornoz*
Centro de Investigación y Docencia Económicas A.C. - CIDE (México)

Recibido: 28 de mayo de 2021 | Aprobado: 06 de mayo de 2022

How to cite: Albornoz, María Mercedes. "Expansión del ámbito territorial de aplicación de la ley en materia de protección de datos personales: ¿Tendencia en América Latina?". *Latin American Law Review*. n.º 09 (2022): 139-160, doi: https://doi.org/10.29263/lar09.2022.08

Resumen

El estudio objeto de este artículo consistió en comprobar que la tendencia a la expansión del ámbito territorial de aplicación de la ley en materia de protección de datos personales existe en América Latina y que en su desarrollo ha recibido la influencia del modelo europeo. Para ello, se realizó un análisis comparativo entre los criterios de aplicabilidad establecidos en la normativa de la Unión Europea, los retenidos por los estándares iberoamericanos y la legislación vigente en los doce Estados de América Latina que cuentan con una ley general sobre protección de datos personales aplicable al tratamiento efectuado por particulares. Asimismo, se exploró el papel de algunos criterios descartados en Europa, pero vigentes en Latinoamérica.

Palabras clave

Protección de datos personales, ámbito territorial, extraterritorialidad, América Latina.

* Doctora en Derecho, Université Panthéon-Assas, Paris II, Francia. Profesora investigadora del Centro de Investigación y Docencia Económicas (CIDE), México. https://orcid.org/0000-0002-0205-4964, ✉ mercedes.albornoz@cide.edu.

Expansion of the Territorial Scope of Application of the Law on the Protection of Personal Data: A Trend in Latin America?

Abstract

The objective of this article is to verify that the trend towards the expansion of the territorial scope of application of the law on personal data protection exists in Latin America and that its development has been influenced by the European model. To achieve this, a comparative analysis of different applicability criteria is carried out in this paper. The legal instruments considered are those of the European Union, the Ibero-American Standards, and the legislation in force in the twelve Latin American States that have a general law on the protection of personal data applicable to the processing by private subjects. In addition, the role of some criteria discarded in Europe but in force in Latin America is explored.

Keywords

Personal data protection, territorial scope, extraterritoriality, Latin America

INTRODUCCIÓN

El flujo de datos personales es potenciado por Internet, cuyo carácter transnacional[1] permite que las comunicaciones virtuales de datos referidos a un individuo identificado o identificable no se detengan en las fronteras estatales. Ahora bien, toda transmisión de datos personales debería estar sujeta a un marco jurídico que garantice la protección del individuo titular de estos. No obstante, debido a concepciones disímiles sobre la protección de datos personales y su regulación[2], aún no existe un instrumento vinculante de alcance universal suscripto por la totalidad o por la mayor parte de los Estados de la comunidad internacional[3] ni tampoco un órgano con jurisdiccional internacional en la materia.

En la actualidad es frecuente que los gigantes tecnológicos, por ejemplo, los de California, Estados Unidos, que desarrollan plataformas y aplicaciones utilizadas por usuarios de muchos países, traten masivamente datos personales de estos sin contar con establecimientos en los Estados donde dichas personas residen. Cuando la legislación de uno de tales Estados condiciona su aplicabilidad a la existencia de un establecimiento del responsable del tratamiento en su territorio, el usuario que sufre una vulneración del derecho a la protección de sus datos personales puede verse privado de acceso efectivo a la justicia y de la aplicación

1 Bertrand de la Chapelle y Paul Fehlinger, "Jurisdiction on the Internet: from Legal Arms Race to Transnational Cooperation," *Internet & Jurisdiction Paper* (2016): 7, https://bit.ly/3u8Yr4Z.

2 Dário Moura Vicente y Sofia de Vasconcelos Casimiro, "Data Protection in the Internet: General Report," en *Data Protection in the Internet*, editado por Dário Moura Vicente y Sofia de Vasconcelos Casimiro (Cham: Springer, 2020), 3-7.

3 El Convenio para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal", del Consejo de Europa del 28 de enero de 1981 (Convenio 108, https://rm.coe.int/16806c1abd), cuya proyección se extiende a los Estados miembros del Consejo de Europa, cinco de África y tres de América Latina –Argentina, México y Uruguay–, dista de tener alcance mundial.

de la ley protectora de su país de residencia. La empresa responsable del tratamiento de los datos personales alegará que su establecimiento se ubica en el extranjero, si le conviene evitar la aplicación de la ley del país donde reside el usuario.

En este contexto, mientras se avanza en la búsqueda de convergencias globales, los Estados que regulan el tema y que se preocupan por proteger los datos personales de su población tienden a actuar unilateralmente expandiendo el alcance de su normativa más allá de las fronteras propias. De este modo, aspiran a abarcar actividades que se despliegan en la esfera virtual. Por tanto, es pertinente preguntarse si esa tendencia a la expansión del ámbito espacial de aplicación de la legislación tuitiva existe también en América Latina.

El ejemplo paradigmático de la tendencia a la extraterritorialidad es el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo del 27 de abril de 2016 (Reglamento General de Protección de Datos –RGPD)[4]. Más apropiado para la era digital que su antecesora —la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 (Directiva)[5]—, el RGPD considera irrelevantes como criterios para determinar su ámbito de aplicación el lugar tanto del tratamiento como de donde se sitúan los datos y los medios empleados para tratarlos.

Internacionalmente, se reconoce que la normativa europea relativa a la protección de datos personales inspiró legislaciones de distintas regiones del mundo, incluyendo las de muchos países de América Latina[6]. No obstante, cabe preguntarse si la influencia de Europa también se verifica en Latinoamérica, en particular, con respecto a la extensión del ámbito territorial de aplicación de la ley.

Además, corresponde tener presente el arraigo de la noción de territorialidad en América Latina. Ante tal circunstancia, también es apropiado cuestionarse acerca del papel que tienen en esta región los criterios del lugar del tratamiento, la localización de los datos y la ubicación de los medios, descartados por el RGPD en su afán de adaptación a la tecnología digital.

En este trabajo se asevera que la tendencia a la expansión del ámbito territorial de aplicación de la ley en materia de protección de datos personales existe en América Latina y que se ha nutrido con el influjo de la normativa europea. Igualmente se sostiene que, sin embargo, la influencia del modelo transatlántico hasta ahora no ha impedido que los criterios del lugar donde se lleva a cabo el tratamiento de los datos, de la localización de estos y de la ubicación de los medios empleados para tratarlos sigan vigentes en la región.

En el estudio que recoge este artículo se comprueba que existe en América Latina la tendencia a la expansión del ámbito territorial de aplicación de la ley y que en su desarrollo ha incidido el modelo europeo. Para ello, se analiza la dogmática jurídica que compara los criterios de aplicabilidad establecidos por la normativa de la Unión Europea (UE) con los consagrados por un instrumento regional de derecho blando (*soft law)* y por la legislación vigente

---

4 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. *Diario Oficial de la Unión Europea*, 4 de mayo de 2016, https://bit.ly/3fs05ui.

5 Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, *Diario Oficial* n.º L 281 de 23 de noviembre de 1995, https://bit.ly/3g4PJjl.

6 "Informe sobre la situación regional 2020," *Internet & Jurisdiction Policy Network*, 2021, 88-90, https://bit.ly/3u8Br63.

en los doce Estados latinoamericanos que cuentan actualmente con una ley general sobre protección de datos personales aplicable al tratamiento efectuado por particulares: Argentina, Brasil, Chile, Colombia, Costa Rica, Ecuador, México, Nicaragua, Panamá, Perú, República Dominicana y Uruguay[7].

El artículo se divide en cuatro partes. La primera contiene precisiones iniciales acerca de la expansión del ámbito espacial de aplicación de la ley. Las tres partes siguientes se concentran en las normas que determinan el ámbito territorial de aplicación en el modelo europeo, en los Estándares de Protección de Datos Personales para los Estados Iberoamericanos (Estándares)[8] y en la legislación de diferentes países de América Latina. Finalmente, se presentan las conclusiones extraídas.

1. PRECISIONES INICIALES

Con respecto a la noción de extraterritorialidad, Kuner señala que no existe una definición única, ampliamente aceptada, de jurisdicción extraterritorial, lo que en gran medida se debe a que su significado varía de un sistema jurídico a otro[9]. En el presente artículo no se retoma la discusión acerca del concepto, sino que se opta por la solución pragmática de considerar como extraterritorial la aplicación de la ley de determinado Estado a personas, bienes que se encuentran en el exterior, o actividades realizadas fuera de sus fronteras.

La extraterritorialidad así definida coincide con lo que Scott denomina "extensión territorial": la aplicación depende de una conexión territorial relevante, pero se debe tomar en cuenta una conducta o circunstancias del extranjero[10]. Como lo apuntan Ryngaert y Taylor al referirse a la aplicación extraterritorial del RGPD, esta "está basada en la territorialidad y es activada por el vínculo territorial de una actividad o persona con la UE"[11]. Por medio de la extensión o expansión del ámbito territorial de aplicación de la ley en materia de datos personales, un Estado decide de manera unilateral que sus normas deben ser aplicadas extraterritorialmente a personas, bienes o actividades realizadas en el extranjero. Nótese que este artículo se enfoca en la extraterritorialidad relativa a la determinación de la aplicabilidad de

---

7 No se incluye Trinidad y Tobago, dado que solo algunas partes de su *Data Protection Act N.º 13 of 2011* entraron en vigor y en ellas no se encuentra la sección 69 sobre el ámbito territorial de aplicación. Véase Tenth Parliament Republic of Trinidad and Tobago, https://www.ttparliament.org/wp-content/uploads/2022/01/a2011-13.pdf y *Legal Notice N.º 2, of 2012*, Republic of Trinidad y Tobago, https://bit.ly/34u3QsJ. Tampoco se incluye Paraguay, a pesar de contar con una ley relativamente reciente, porque su alcance se limita a la protección en materia de datos personales crediticios. Véase Ley 6534 de Protección de Datos Personales Crediticios, *Gaceta Oficial de la República del Paraguay*, 28 de octubre de 2020, http://www.gacetaoficial.gov.py/index/getDocumento/65863.

8 Adoptados por la Red Iberoamericana de Protección de Datos –RIPD– en 2017, con base en el texto redactado por Nelson Remolina Angarita, https://www.redipd.org/es/documentos/estandares-iberoamericanos.

9 Christopher Kuner, "Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law," *International Data Privacy Law* 5, n.° 4 (2015): 238.

10 Joanne Scott, "Extraterritoriality and Territorial Extension in EU Law," *American Journal of Comparative Law* 62, n.° 1 (2014): 90.

11 Cedric Ryngaert y Mistale Taylor, "The GDPR as *Global* Data Protection Regulation?," *AJIL Unbound* 114 (2020): 6, https://bit.ly/3ykAv1X.

la legislación y no en el régimen específico de las comunicaciones transfronterizas de datos personales. Aunque el segundo tiene impacto fuera del territorio, solo será aplicado una vez que se hayan cumplido los criterios establecidos para la primera.

Por otro lado, la extensión del ámbito territorial de aplicación de la ley es un tema de derecho aplicable. Si bien jurisdicción y derecho aplicable son conceptos diferentes, están interrelacionados y en materia de protección de datos personales tienden a coincidir[12], a lo cual contribuye "la estricta correlación entre ley aplicable y autoridad competente característica del ámbito administrativo"[13]. En consecuencia, las normas sobre derecho aplicable estudiadas en el presente texto pueden servir para la determinación de la competencia[14]. De modo que no es inusual que en materia de datos personales se extraiga de ellas conclusiones de carácter jurisdiccional[15], ni sorprende que Kuner considere más práctico, en este ámbito, utilizar "ley aplicable" y "jurisdicción" como sinónimos[16].

Por último, se debe aclarar que la intención de extender en el espacio el ámbito de aplicación de la legislación propia sobre datos personales no es exclusiva de regímenes generales como el de la UE. También se la percibe en países con estándares divergentes en esta materia como Estados Unidos, donde la regulación tiene carácter sectorial[17]. Pero el esquema de delimitación del alcance territorial utilizado a nivel europeo ha llamado poderosamente la atención en otras latitudes[18].

2. NORMATIVA EUROPEA

Desde la perspectiva europea, plasmada en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea del 7 de diciembre de 2000[19], el derecho a la protección de datos de carácter personal es un derecho fundamental. Empero, desde un lustro antes ya existía la Directiva como instrumento jurídico específico sobre el tema. Dos décadas después, esta fue derogada y sustituida por el RGPD, aplicable desde el 25 de mayo de 2018.

---

12 Kuner, "Extraterritoriality and Regulation", 236.

13 Pedro Alberto de Miguel Asensio, "Competencia y derecho aplicable en el Reglamento General sobre Protección de Datos de la Unión Europea," *Revista Española de Derecho Internacional* 69, n.° 1 (2017): 78.

14 Así lo entiende De Miguel Asensio con respecto al artículo 3 del RGPD cuando, para cuestiones no unificadas por él, hay que decidir la ley de qué Estado miembro de la UE aplicar. *Ibid.*, 79.

15 Esto ocurre en Colombia, como lo explica Nelson Remolina en *Recolección internacional de datos personales: un reto del mundo post-internet* (Madrid: Agencia Española de Protección de Datos - Agencia Estatal Boletín Oficial del Estado, 2015), 350.

16 Kuner, "Extraterritoriality and Regulation", 236.

17 Acerca del ámbito de aplicación de la Ley de Protección de la Privacidad Infantil en Línea (COPPA), véase Adèle Azzi, "The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation," *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 9, n.° 2 (2018): 132.

18 Dan Jerker B. Svantesson, "The Extraterritoriality of EU Data Privacy Law - Its Theoretical Justification and Its Practical Effect on U.S. Businesses," *Stanford Journal of International Law* 50, n.° 1 (2014): 61.

19 Carta de los Derechos Fundamentales de la Unión Europea, del 7 de diciembre de 2000, *Diario Oficial de la Unión Europea*, 7 de junio de 2016, https://bit.ly/3foFtmE.

El ámbito espacial de aplicación del derecho de los Estados miembros fue regulado en el artículo 4 de la Directiva y en el artículo 3 del RGPD. Ambas normas tienen un esquema tripartito y coinciden en dos de los criterios que establecen. Sin embargo, con respecto al otro criterio, se aprecia una evolución en el RGPD.

2.1. Establecimiento en el territorio de la Unión Europea

El primer criterio para determinar el ámbito territorial de aplicación del RGPD es el de la ubicación en la Unión de un establecimiento del responsable o del encargado del tratamiento de datos personales. Según el artículo 3.1. del RGPD, este "se aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no".

En cuanto a la noción de "establecimiento", el considerando 22 del RGPD precisa que "implica el ejercicio de manera efectiva y real de una actividad a través de modalidades estables", sin que importe la forma jurídica que dichas modalidades adopten. También se debe subrayar la irrelevancia del lugar del tratamiento y de la ubicación de los interesados. Lo que importa es que el tratamiento de datos personales de personas físicas, "independientemente de su nacionalidad o de su lugar de residencia" —considerando 14—, se realice en el contexto de las actividades de un establecimiento en la UE. Con respecto a esto último, el Comité Europeo de Protección de Datos (CEPD) explica que no es indispensable que el tratamiento sea realizado por el establecimiento del responsable o del encargado situado en territorio de la Unión[20].

2.2. Del recurso a medios situados en el territorio al *targeting* de interesados que se encuentren en la Unión Europea

2.2.1. Recurso a medios situados en el territorio de la Unión Europea

En ausencia de establecimiento en el territorio comunitario, en el artículo 4 de la Directiva se establecía el criterio del recurso a medios —automatizados o no— situados en el territorio de un Estado miembro, para efectuar el tratamiento de datos personales. En tal caso, el tratamiento quedaba sometido al derecho nacional de ese Estado miembro, excepto si esos medios solo eran utilizados con fines de tránsito. Además, se indicaba que cuando el responsable establecido en un tercer Estado recurriese a medios ubicados en el territorio de un Estado miembro, debía designar un representante establecido allí. Kuner señala que el uso de la palabra *"equipment"* en el artículo 4 —traducida como "medios" en la versión en español[21]— pone en evidencia que la Directiva se originó antes de que Internet comenzara a ser tan popular como hoy[22].

---

20 "Directrices 3/2018 relativas al ámbito territorial del RGPD (artículo 3), versión 2.1," Comité Europeo de Protección de Datos [CEPD], 12 de noviembre de 2019, 8, https://bit.ly/3yxGO2f.

21 El Grupo de Trabajo del Artículo 29 promueve una interpretación amplia y entiende el término *equipment* como "medios". Dictamen 8/2010 sobre derecho aplicable, 16 de diciembre de 2010, https://bit.ly/3yqxtZS.

22 Christopher Kuner, "Data Protection Law and International Jurisdiction on the Internet (Part. 2)," *International Journal of Law and Information Technology* 18, n.° 3 (2010): 228.

El objetivo de la norma era no incentivar a los responsables del tratamiento a eludir la aplicación de la ley localizando su establecimiento en otra región. Empero, la Directiva no ofrecía pautas de interpretación. Incluso, el Grupo de Trabajo del Artículo 29 reconoció que se requería una evaluación caso por caso y consideró que la recolección de datos personales, por parte de responsables establecidos en terceros países empleando *cookies* instaladas en computadoras de los usuarios, podría desencadenar la aplicación de esta norma[23], lo que generó controversias[24]. Por tanto, algunos tratamientos carentes de una fuerte proximidad con la UE podían resultar sometidos al derecho de un Estado miembro.

A la falta de certeza y la excesiva extensión del ámbito de aplicación de la legislación europea se sumaron los avances tecnológicos de la era digital, para reforzar la idea de que la mera localización de medios a los cuales se recurre a fin de tratar datos personales no era un criterio apropiado para proteger la información de interesados que se encontraban en la UE. Esta preocupación fue atendida en el RGPD, que sustituyó la ubicación de los medios por un nuevo criterio: *targeting*, focalización o "direccionamiento".

2.2.2. *Targeting*

El artículo 3.2 del RGPD es una norma internacionalmente imperativa[25], que determina la aplicación del Reglamento a casos internacionales con un vínculo territorial singular con la UE. Busca garantizar la protección de los interesados que se encuentren en su territorio[26] en el momento del tratamiento y cuyos datos personales sean tratados por un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con la oferta de bienes o servicios a dichos interesados en el territorio de la UE, o con el control de su comportamiento, siempre y cuando este último tenga lugar en la UE. A diferencia de lo que establece el artículo 3.1, en el 3.2 es importante la ubicación de los titulares.

A fin de que la oferta de bienes o servicios se encuadre en esta norma, el responsable o encargado debe tener la intención de ofrecerlos a titulares que se encuentren en la UE. Para la detección de esa intención, independientemente de si se les exige a los interesados el pago de una suma de dinero como contraprestación, el considerando 23 enuncia diversos factores que pueden ser útiles al valorar las circunstancias de cada caso.

Con respecto al control del comportamiento, se requiere que la recolección de información personal se haga con la intención de tratarla y, especialmente, de utilizarla como insumo de la creación de perfiles o de la aplicación de otras técnicas de análisis del comportamiento[27].

---

23 Grupo de Trabajo del Artículo 29, Dictamen 8/2010.

24 Kuner, "Data Protection Law", 229.

25 En este sentido, Marian Thon, "Transnationaler Datenschutz: Das Internationale Datenprivatrecht der DS-GVO," *Rabels Zeitschrift für ausländisches und internationales Privatrecht* 84, n.° 1 (2020): 41.

26 La versión en español que en su momento fue publicada en el Diario Oficial de la Unión Europea indica "interesados que residan en la Unión". El error de traducción del inglés al español fue corregido poco después, quedando claro que la redacción correcta es "interesados que se encuentren en la Unión", *Diario Oficial de la Unión Europea*, 23 de mayo de 2018, https://bit.ly/3vqPbKQ.

27 Directrices 3/2018 relativas al ámbito territorial del RGPD, 22.

Es habitual que los usuarios de Internet sean objeto de seguimiento mientras navegan en la red. Del considerando 24 se infiere que este control pone en riesgo la autonomía de los individuos.

Asimismo, el artículo 27 instaura la obligación del responsable o el encargado, establecido en un tercer Estado, de designar por escrito un representante en la Unión, en uno de los Estados miembros donde se encuentren los interesados destinatarios de la oferta de bienes o servicios o cuyo comportamiento es objeto de control. Esto no significa que desde entonces tenga un establecimiento en la Unión[28].

La sustitución de la localización de los medios utilizados para el tratamiento de datos personales por el criterio del *targeting* merece una valoración positiva como esfuerzo de adaptación a la era digital. Sin embargo, se ha observado que los contornos de la noción de *targeting* no están del todo definidos, lo que exige hacer un análisis caso por caso, con el consiguiente riesgo de incertidumbre para las partes[29]. Se pone de relieve aquí el consabido reto de lograr un equilibrio entre seguridad jurídica y justicia material, entre puntos de conexión rígidos y puntos de conexión flexibles[30].

2.3. Aplicación en virtud del derecho internacional público

El artículo 3.3 del RGPD dispone que el "Reglamento se aplica al tratamiento de datos personales por parte de un responsable que no esté establecido en la Unión sino en un lugar en que el Derecho de los Estados miembros sea de aplicación en virtud del Derecho internacional público". El CEPD entiende que queda comprendido en el ámbito de aplicación del RGPD el tratamiento de datos personales efectuado por embajadas y consulados de los Estados miembros de la Unión ubicados en terceros países[31].

Una vez presentada y analizada la normativa europea relativa a la determinación del ámbito espacial de aplicación del régimen sobre protección de datos personales vigente en la UE, se hará lo propio con los Estándares de Protección de Datos Personales para los Estados Iberoamericanos (Estándares), instrumento de derecho blando adoptado en 2017 por la Red Iberoamericana de Protección de Datos.

3. ESTÁNDARES IBEROAMERICANOS

Los Estándares son un instrumento de derecho blando que reúne un conjunto de principios y derechos de protección de datos personales, destinados a orientar a los Estados de Iberoamérica cuando reformen su legislación sobre el tema, "con la finalidad de garantizar el debido

---

28 De lo contrario, quedaría comprendido en el supuesto del artículo 3.1 del RGPD.

29 "Internet & Jurisdiction Global Status Report 2019", *Internet & Jurisdiction Policy Network*, 2019, 149, https://bit.ly/3fGKgPw.

30 Véase Julio D. González Campos, "Diversification, spécialisation, flexibilisation et matérialisation des règles de Droit international privé". *Recueil des cours de l'Académie de Droit International de La Haye* 287 (2000): 9-426.

31 Directrices 3/2018 relativas al ámbito territorial del RGPD, 25.

tratamiento de los datos personales y contar con reglas homogéneas en la región" —artículo 1.1.a—. Aunque no son el único instrumento de este tipo, dado que el Comité Jurídico Interamericano de la Organización de los Estados Americanos adoptó un cuerpo de Principios sobre la Privacidad y la Protección de Datos Personales[32], solo los Estándares contienen normas sobre el ámbito territorial de aplicación.

Los Estándares tienden un puente entre el RGPD y los Estados de América Latina. En el considerando 8 reconocen la importancia del nuevo marco normativo de la UE. Con respecto al ámbito territorial de aplicación, es necesario examinar si se verifica la tendencia a la expansión y, además, si se percibe la influencia del RGPD en los Estándares en esta área —especialmente, en los cuatro supuestos del artículo 5.1—.

En primer lugar, queda comprendido en el ámbito territorial de aplicación de los Estándares el tratamiento de datos personales efectuado "por un responsable o encargado establecido en territorio de los Estados Iberoamericanos" —artículo 5.1.a—. Este criterio puede haber sido inspirado por el artículo 3.1 del RGPD. Ambas normas tienen en común el punto de conexión "establecimiento" como vínculo con el territorio; la inclusión no solo del responsable, sino también del encargado del tratamiento; y el reconocimiento —expreso en el RGPD e implícito en los Estándares— de que para estos efectos no importa el lugar del tratamiento. Sin embargo, también hay diferencias: en los Estándares no se exige que el tratamiento sea realizado en el contexto de las actividades del establecimiento y tampoco se indica que puede tratarse de "un" establecimiento —admitiendo la posibilidad de que haya varios—, como lo hace el RGPD.

En los tres supuestos restantes, el responsable o encargado no está establecido en un Estado iberoamericano. Se comienza con el criterio del *targeting* en el artículo 5.1.b. En esta norma es evidente la impronta del artículo 3.2 del RGPD. No obstante, el artículo de los Estándares no contiene la siguiente frase del artículo 3.2 del RGPD: "Independientemente de si a éstos se les requiere su pago". De todos modos, esta ausencia no es importante, ya que en ambos el hecho de que a los titulares o interesados se les requiera o no un pago por los bienes o servicios ofrecidos es, simplemente, uno más de los factores a ser sopesados en el caso concreto. En cambio, hay una divergencia más relevante: mientras el artículo 5.1.b de los Estándares requiere que los titulares de los datos objeto de tratamiento sean residentes de los Estados iberoamericanos, para el artículo 3.2 del RGPD basta con que se encuentren en la Unión. Por tanto, excepto sobre este punto específico, los criterios de interpretación del RGPD plasmados en sus considerandos, en directrices del CEPD y en decisiones de las autoridades competentes en materia de *targeting*, deberían ser tomados en cuenta para interpretar el artículo 5.1.b de los Estándares.

A continuación, en virtud del artículo 5.1.c de los Estándares, el tratamiento de datos personales efectuado por un responsable o encargado no establecido en un Estado iberoamericano queda sometido a estos, si le resulta aplicable la legislación nacional de un Estado iberoamericano como consecuencia de "la celebración de un contrato o en virtud del derecho internacional público". La aplicación de la ley de cierto Estado en estas circunstancias, porque así lo dispone el derecho internacional público, está prevista en la normativa de la UE —artículo 3.3, RGPD—. En cambio, no ocurre lo mismo con la celebración de un contrato como

32 Aprobados en 2015 y actualizados en 2021, https://bit.ly/3i3iIXn.

fundamento de la aplicación de determinada legislación nacional, criterio que, como se verá más adelante, está presente en las leyes de Costa Rica[33], México y Perú[34].

Finalmente, los Estándares añaden el supuesto del responsable o encargado no establecido en territorio de los Estados iberoamericanos, que "utilice o recurra a medios, automatizados o no, situados en ese territorio para tratar datos personales, salvo que dichos medios se utilicen solamente con fines de tránsito" —artículo 5.1.d—. Esta norma es prácticamente idéntica a la contenida en el artículo 4 de la Directiva. Recuérdese que este criterio de la Directiva fue sustituido por el del *targeting* en el RGPD. Puede llamar la atención que los Estándares, siendo posteriores a esa evolución en la UE, adopten un criterio que fue juzgado poco adecuado para la era digital. Empero, lo incorpora como alternativo a otros, entre los cuales se encuentra el del *targeting*. Una razón que podría explicar la inclusión en los Estándares de la localización de los medios es el peso que tradicionalmente ha tenido el territorialismo en Latinoamérica[35], reflejado también en la consagración de este criterio en las legislaciones de México, Perú[36] y Uruguay[37].

4. LEGISLACIÓN DE ESTADOS DE AMÉRICA LATINA

En esta sección se analiza el tema del presente artículo en doce países de la región. Al abordar algunos Estados donde la situación es muy similar a la de otros, se los agrupa en un mismo apartado. Ello sucede cuando el legislador guarda silencio acerca de la aplicación de la ley a responsables establecidos fuera del territorio nacional (4.1), o cuando las normas de un país sobre esta cuestión fueron tomadas casi literalmente de otro (4.6). En el resto de los casos, se dedica un apartado a cada Estado.

4.1. Argentina, Chile, Nicaragua y República Dominicana

Con respecto al ámbito espacial de aplicación de su legislación en materia de datos personales, estos cuatro países tienen en común la ausencia de reglas que lo delimiten expresamente, considerando la posibilidad de que el tratamiento sea efectuado por sujetos establecidos en el extranjero.

En Argentina, la Ley 25326 de Protección de los Datos Personales data del año 2000[38]. El artículo 44 se limita a indicar cuáles de sus normas son de orden público y de aplicación en todo el territorio nacional. Sin embargo, cabe mencionar dos proyectos argentinos para

---

33 Véase *infra*, 4.4.

34 Véase *infra*, 4.6.

35 Véase Leonel Pereznieto Castro, "La tradition territorialiste en droit international privé dans les pays d'Amérique Latine," en *Recueil des cours de l'Académie de Droit International de La Haye* (1985): 190.

36 Véase *infra*, 4.6.

37 Véase *infra*, 4.8.

38 *Boletín Oficial*, 2 de noviembre de 2000, https://bit.ly/2QXaWmx.

sancionar una ley moderna en la materia. Uno de ellos[39] regula el ámbito espacial de aplicación de modo muy similar a como lo hace el RGPD. El otro incorpora el criterio flexible de la ley más favorable al titular de datos personales residente en Argentina, lo que resulta innovador en esta área del derecho. Implica considerar al titular como parte débil merecedora de protección[40] y consiste en permitirle optar por la aplicación de la ley extranjera del lugar donde se encuentra el responsable del tratamiento, cuando dicha ley sea más favorable a su propia protección[41].

La ley chilena en esta materia es la Ley 19628 sobre Protección de la Vida Privada, de 1999[42], ninguno de cuyos artículos determina el ámbito territorial de aplicación de la normativa ni ofrece pautas suficientes para inferirlo. El Código Civil de Chile[43] dispone que "la ley es obligatoria para todos los habitantes de la República, incluso los extranjeros" —artículo 14—, mas no resulta de gran ayuda para inferir, por ejemplo, en qué circunstancias el tratamiento de datos personales efectuado por gigantes tecnológicos establecidos fuera de Chile será regido por la ley nacional.

Nicaragua y República Dominicana cuentan con leyes mucho más recientes que la argentina y la chilena. Sin embargo, la Ley 787 de Protección de Datos Personales de Nicaragua, de 2012[44], no contiene una delimitación específica de su ámbito territorial de aplicación. Tan solo el artículo 32, sobre procedimientos de inspección, alude a la inspección de ficheros de datos dentro del territorio nicaragüense. En cuanto a República Dominicana, el artículo 3 de la Ley 172 sobre la Protección Integral de los Datos Personales, de 2013[45], simplemente dispone que sus normas "son de orden público y de aplicación en todo el territorio nacional", tal como sucede en la ley vigente en Argentina.

Sería beneficioso para la protección de los titulares de datos personales que en Argentina, Chile, Nicaragua y República Dominicana la legislación delimitara en forma expresa su ámbito de aplicación, especialmente en lo atinente al tratamiento de datos personales efectuado a través de Internet.

4.2. Brasil

La situación de la legislación sobre protección de datos personales en Brasil es singular. Por un lado, la Ley 12965 de 2014 que establece el Marco Civil de Internet[46] contiene algunas normas sobre el tema y, por otro lado, en 2018 se aprobó la Ley 13709, Ley General de Protección de

39 Proyecto de ley 6234-D-2020, https://bit.ly/3uttkRL.

40 Véase María Mercedes Albornoz, "El titular de datos personales, parte débil en tiempos de auge de la Inteligencia Artificial. ¿Cómo fortalecer su posición?," *Revista Ius* 15 n.° 48 (2021): 209-242, https://www.revistaius.com/index.php/ius/article/view/715/798.

41 Proyecto de ley 2986-S-20020, https://www.senado.gob.ar/parlamentario/comisiones/verExp/2986.20/S/PL.

42 *Biblioteca del Congreso Nacional de Chile*, 28 de agosto de 1999, http://bcn.cl/2owi8.

43 Texto refundido, coordinado y sistematizado del Código Civil y otras leyes, 16 de mayo de 2000, *Biblioteca del Congreso Nacional de Chile,* http://bcn.cl/1uu74.

44 *La Gaceta Diario Oficial*, 29 de marzo de 2012, https://bit.ly/3bPTkAd.

45 *Gaceta Oficial*, 15 de diciembre de 2013, https://bit.ly/3fNVVMb.

46 *Presidencia de la República*, 23 de abril de 2014, https://bit.ly/3wIwLpn.

Datos Personales[47], que lo regula de manera integral con criterios inspirados en el RGPD. El enfoque adoptado en ambas leyes a fin de determinar cuándo corresponde aplicar el derecho brasileño tiene un marcado corte territorialista. Dicho esto, considerando que la segunda ley es especial con respecto a la primera en materia de datos personales[48], a continuación se pone el foco en la más reciente.

El ámbito territorial de aplicación de la Ley General de Protección de Datos Personales se determina en función de los criterios establecidos en su artículo 3, que en el primer párrafo dispone:

> Esta ley se aplica a cualquier operación de tratamiento realizada por persona natural o por persona jurídica de derecho público o privado, independientemente del medio, del país de su sede o del país donde estén localizados los datos, siempre que:
>
> I. la operación de tratamiento sea realizada en el territorio nacional[49];
>
> II. la actividad de tratamiento tenga por objetivo la oferta o el suministro de bienes o servicios o el tratamiento de datos de individuos localizados en el territorio nacional; o
>
> III. los datos personales objeto del tratamiento hayan sido recolectados en el territorio nacional[50].

Se advierte el interés en expandir el ámbito de aplicación de la legislación brasileña. Asimismo, en comparación con el artículo 3 del RGPD, el legislador de Brasil desechó el criterio del establecimiento del responsable o del encargado en su territorio y la aplicación de la ley en virtud del derecho internacional, y solo rescató el *targeting*, pero lo reguló con matices propios. Por tanto, se destaca la irrelevancia del país de localización de los datos y de aquel donde se ubique la sede de quien efectúa la operación de tratamiento. En cambio, el artículo 3 de la ley brasileña le asigna gran relevancia al lugar de realización del tratamiento en territorio nacional —inciso I—. Ahora bien, no queda clara la utilidad del inciso III sobre recolección de los datos en Brasil si se considera que esta última es una operación de tratamiento según el artículo 5, inciso X de la misma ley.

Por otro lado, el criterio del *targeting* fue incorporado en el inciso II del artículo 3 con particularidades que lo distinguen del modelo europeo. Las más importantes son dos: no se requiere que el *targeting* sea efectuado por un sujeto establecido fuera de Brasil y, en lugar de

---

47 *Presidencia de la República*, 15 de agosto de 2018, https://bit.ly/3bZ6ZVF.

48 Leonardo Parentoni y Henrique Cunba Souza Lima, "Proteção de Dados Pessoais no Brasil: Antinomias Internas e Aspectos Internacionais", en *Direito & Internet IV. Sistema de Proteção de Dados Pessoais*, coordinado por Newton de Lucca *et al*. (San Pablo: Quartier Latin, 2019), 492.

49 No obstante, queda exceptuado de lo dispuesto en el inciso I el tratamiento de datos personales "provenientes de fuera del territorio nacional y que no sean objeto de comunicación, uso compartido de datos con agentes de tratamiento brasileños u objeto de transferencia internacional de datos con otro país que no sea el de proveniencia, siempre que el país de proveniencia proporcione un grado de protección de datos personales adecuado a lo previsto en esta Ley" –artículo 4.IV–.

50 El mismo artículo 3 aclara que "se consideran recolectados en el territorio nacional los datos personales cuyo titular se encuentre en él en el momento de la recolección".

prever específicamente el control del comportamiento como uno de los objetivos del direccionamiento, se alude al "tratamiento" de datos de individuos localizados en territorio nacional, cuyo alcance es mucho más amplio. De esta manera, queda comprendido en el ámbito de aplicación de la ley brasileña cualquier tratamiento de datos personales de un individuo que se encuentre en Brasil, efectuado en el extranjero por una empresa domiciliada en el extranjero. En este sentido, el brazo de la ley llegaría más lejos que el del RGPD.

4.3. Colombia

En Colombia, el régimen general para la protección de datos personales fue establecido por la Ley Estatutaria 1581 de 2012[51]. De conformidad con el párrafo segundo del artículo 2, esta ley se aplicará "al tratamiento de datos personales efectuado en territorio colombiano o cuando al Responsable del Tratamiento o Encargado del Tratamiento no establecido en territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales".

La ley le confiere un fuerte peso al hecho de que el tratamiento se realice en territorio nacional. Aunque a primera vista podría parecer lo contrario, esto no implica ausencia de apetito de expansión de su alcance territorial. La clave está en que el concepto de tratamiento es amplio: comprende la recolección de datos personales —tal como expresamente lo indica el artículo 3, inciso g) de la ley—; puede realizarse a través de cualquier herramienta, tecnología o proceso; y puede ser efectuado por un responsable o encargado domiciliado en Colombia o en el exterior. En este sentido, la autoridad nacional de protección de datos ha considerado que la recolección de datos en territorio colombiano empleando *cookies,* realizada por empresas extranjeras como Facebook[52], Google[53] y WhatsApp[54] queda comprendida en el ámbito de aplicación de la ley colombiana. Asimismo, ha explicitado que:

> Para recolectar y tratar datos en Colombia no es necesario estar domiciliado en este país. Avances y herramientas tecnológicas permiten que empresas u organizaciones recolecten datos en Colombia sin hacer presencia física en nuestro territorio. Estas organizaciones realizan "presencia tecnológica" en nuestro territorio mediante el uso de las citadas herramientas o aplicativos que se instalan en los equipos (teléfonos, tabletas, computadores, etc.) ubicadas en el territorio colombiano. Esa realidad no puede desconocerse ni ser argumento para eximirse de la aplicación de la regulación colombiana[55].

---

51 *Secretaría del Senado*, 18 de octubre de 2012, https://bit.ly/3hWj2a8.

52 Resolución 12192, 1 de abril de 2020, https://www.sic.gov.co/sites/default/files/files/2020/Res%2012192%2001IV2020%20SIC%20Facebook%20Inc.pdf.

53 Resolución 2389, 28 de enero de 2022, https://www.sic.gov.co/sites/default/files/documentos/022022/Resolucion2389-de-28-de-enero-de-2022_GoogleLLC.pdf.

54 Resolución 15342, 28 de marzo de 2022, https://www.sic.gov.co/sites/default/files/documentos/042022/Resolucion-15342-de-28-marzo-de-2022_WhatsApp-LLC.pdf.

55 Ídem, 48.

Finalmente, al enfocarse en el lugar del tratamiento y no en la ubicación del establecimiento de quien lo realiza, la Ley Estatutaria 1581 se aleja de la normativa europea[56]. Sin embargo, el segundo criterio consagrado por la ley colombiana coincide con la aplicación en virtud del derecho internacional prevista tanto en la Directiva como en el RGPD. En efecto, de la lectura del segundo párrafo del artículo 2 de la ley colombiana se sigue que, en este supuesto, el responsable o encargado no está domiciliado en Colombia y tampoco efectúa allí el tratamiento de datos personales[57], pero se le aplica la ley colombiana porque así lo disponen normas y tratados internacionales.

4.4. Costa Rica

En Costa Rica, el tratamiento de datos personales está regulado por la Ley 8968 de 2011 sobre Protección de la Persona frente al Tratamiento de sus Datos Personales[58]. Aunque el ámbito territorial de aplicación de la ley es delimitado en el decreto reglamentario —Decreto Ejecutivo 37554-JP del 30 de octubre de 2012[59]—, la ley proporciona información importante en relación con la persona física titular de los datos. El artículo 1 establece que la protección en esta materia se le garantiza "a cualquier persona, independientemente de su nacionalidad, residencia o domicilio".

Por su parte, el artículo 3 del Reglamento señala que se aplicará a los datos personales que figuren en las bases de datos y a toda modalidad de uso posterior de aquellos, "en tanto surtan efectos dentro del territorio nacional, o les resulte aplicable la legislación costarricense derivada de la celebración de un contrato o en los términos del derecho internacional". La ausencia de toda indicación sobre la localización del establecimiento de quien realiza el tratamiento permite inferir que esta es irrelevante.

El primer criterio, la producción de efectos en el territorio costarricense, comprende perfectamente los dos tipos de actividades de *targeting* que luego fueron previstas en el artículo 3.2 del RGPD —oferta de bienes y servicios, y control de comportamiento—, por lo que alcanzaría el tratamiento de datos de personas residentes en Costa Rica efectuado por empresas extranjeras a través de Internet. El segundo criterio, la aplicación de la ley nacional como consecuencia de la celebración de un contrato o de los términos del derecho internacional, implícitamente supone que el responsable del tratamiento está domiciliado fuera del territorio costarricense.

4.5. Ecuador

De todos los países latinoamericanos comprendidos en el presente artículo, Ecuador es el que cuenta con legislación más reciente. Su Ley Orgánica de Protección de Datos Personales

---

56 Concretamente de la Directiva, ya que el RGPD es posterior a la Ley Estatutaria 1581.

57 Véase la Resolución 12192 del Superintendente Delegado para la Protección de Datos Personales, 14.

58 *Sistema Costarricense de Información Jurídica*, 5 de septiembre de 2011, https://bit.ly/3oIJyp1.

59 *Sistema Costarricense de Información Jurídica*, 5 de marzo de 2013, https://bit.ly/3bPaCNT.

fue aprobada el 10 de mayo de 2021[60]. El artículo 3 regula el ámbito territorial de aplicación en cuatro incisos, sin perjuicio de lo establecido en instrumentos internacionales ratificados por Ecuador.

El inciso 1 prevé el criterio de la realización del tratamiento en territorio ecuatoriano, que opera independientemente del lugar donde esté establecido el responsable o encargado. El inciso 2, se refiere al domicilio del responsable o encargado del tratamiento en el país. El 3, incorpora el *targeting* de titulares residentes en Ecuador, por parte de un responsable o encargado no establecido en territorio nacional, mediante actividades relacionadas con la oferta de bienes o servicios o con el control del comportamiento. El 4, la aplicación de la legislación nacional al responsable o encargado no domiciliado en Ecuador, en virtud de un contrato o del derecho internacional público.

Se observa que los incisos 2, 3 y 4 del artículo 3 contemplan criterios consagrados por el artículo 3.1 del RGPD, con algunos matices y con el agregado del contrato como fundamento de la aplicación de la ley ecuatoriana. Pero el rasgo más interesante del artículo 3 de la Ley Orgánica de Protección de Datos Personales es que los combina con el lugar del tratamiento, rechazado por la normativa vigente en la UE. Aquí se percibe una tensión a la que se ve expuesto el legislador, entre el peso de la tradición territorialista y la voluntad de adoptar un criterio moderno como el del *targeting*. Sin embargo, si en el inciso 1 se establece el punto de conexión lugar de tratamiento, siendo indistinta la ubicación del establecimiento del responsable o encargado, ya no se justifica añadir el inciso 3 para captar al responsable o encargado establecido fuera del país.

4.6. México y Perú

Estos dos países son abordados en el mismo apartado, debido a que las normas mexicanas referidas a la delimitación del ámbito territorial de aplicación de la ley en esta materia fueron tomadas como fuente directa por el legislador peruano.

En México, el tratamiento de datos personales realizado por particulares es regido por una ley de 2010, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares[61], cuyo ámbito territorial de aplicación se determina en el artículo 4 del Reglamento, expedido en 2011[62]. Esta normativa mexicana tuvo influencia en Perú, donde se percibe la impronta territorialista que ha calado hondo en la región.

En Perú, el artículo 3 de la Ley 29733 de Protección de Datos Personales, de 2011[63], fija la pauta rectora del alcance territorial: esta ley "es de aplicación a los datos personales contenidos o destinados a ser contenidos en bancos de datos personales (…) cuyo tratamiento se realiza en el territorio nacional". El artículo 5 del Decreto Supremo 003-2013-JUS[64], que reglamenta dicha ley, fue tomado de manera prácticamente literal del artículo 4 del Reglamento

60 *Registro Oficial*, 26 de mayo de 2021, https://bit.ly/3wxPDqO.

61 *Cámara de Diputados del H. Congreso de la Unión*, 5 de julio de 2010, https://bit.ly/2SytrxY.

62 *Cámara de Diputados del H. Congreso de la Unión*, 21 de diciembre de 2011, https://bit.ly/34omnHa.

63 *Sistema Peruano de Información Jurídica*, 3 de julio de 2011, https://bit.ly/2SBl4BN.

64 *El Peruano*, 22 de marzo de 2013, https://bit.ly/3vEoiTG.

mexicano. Por eso se hará alusión a la norma de México, en el entendido de que lo que se afirme a continuación también será válido con respecto a Perú.

En primer lugar, se adopta el criterio del lugar de tratamiento en el territorio nacional, atado al de la ubicación de un establecimiento del responsable en el mismo territorio. Se somete a la ley de México el tratamiento "efectuado en un establecimiento[65] del responsable ubicado en territorio mexicano" —artículo 4, fracción I—. En este punto hay un contraste con el artículo 3.1 del RGPD, que no requiere que el tratamiento se haya efectuado en la UE.

Luego se contempla el supuesto del tratamiento realizado "por un encargado con independencia de su ubicación, a nombre de un responsable establecido en territorio mexicano" —artículo 4, fracción II—. En este caso, la relación con el país está dada por la actuación a nombre de un responsable establecido en el territorio nacional. La norma tiene en cuenta que, a los fines de la protección del titular, quien responde es, como su denominación lo indica, el responsable del tratamiento.

En tercer lugar, la ley se aplica al tratamiento realizado por un responsable establecido en el extranjero, siempre que utilice medios situados en el territorio de México, excepto si solo los utiliza con fines de tránsito —artículo 4, fracción IV—. En este criterio se aprecia la huella de la Directiva europea. Adicionalmente, la normativa mexicana establece que, en este supuesto, el responsable tendrá que proveer los medios para cumplir la ley, para lo cual podrá nombrar un representante en México o implementar algún otro mecanismo.

Asimismo, en cuarto lugar, se prevé la aplicación de la ley mexicana al tratamiento hecho por un responsable no establecido en México, a quien aquella obligue en virtud de la celebración de un contrato o en términos del derecho internacional —artículo 4, fracción III—.

Por otro lado, el artículo 4 del Reglamento también dispone que cuando el responsable no se encuentre ubicado en territorio mexicano pero el encargado sí, a este último se le aplicarán las disposiciones sobre medidas de seguridad del mismo reglamento.

Nótese que ni México ni Perú incluyen el criterio del *targeting*, lo cual puede deberse a que sus normas son anteriores al RGPD. Esta ausencia deja un vacío, puesto que en la configuración actual de las reglas sobre determinación del ámbito territorial de aplicación de la ley no hay un supuesto que permita cubrir los casos de tratamiento de datos personales de individuos que se encuentren en México o en Perú, por parte de empresas responsables establecidas en el extranjero, si no se emplean medios ubicados en territorio mexicano o peruano.

4.7. Panamá

El primer párrafo del artículo 5 de la Ley Panameña de Protección de Datos Personales, Ley 81 de 2019[66], dispone: "Las bases de datos que se encuentren en el territorio de la República de Panamá, que almacenen o contengan datos personales de nacionales o extranjeros o que el responsable del tratamiento de los datos esté domiciliado en el país quedan sujetas a las normas establecidas en esta Ley o su reglamentación". Dos son los criterios acogidos: localización de las bases de datos y domicilio del responsable del tratamiento, ambos en Panamá.

---

65 Los párrafos tercero y cuarto del artículo 4 del Reglamento contienen precisiones sobre el establecimiento.

66 *República de Panamá. Asamblea Nacional*, 29 de marzo de 2019, https://bit.ly/34omPVS.

Aunque la redacción de la norma es confusa, se entiende que los criterios son alternativos, por lo que la ley panameña se aplicará a todo responsable del tratamiento de datos personales establecido en el país, así como a los datos personales que allí se encuentren, independientemente de dónde esté domiciliado el responsable de tratarlos. Siguiendo esta línea de razonamiento, los datos personales recolectados en Panamá por empresas extranjeras quedarían sometidos a la legislación panameña[67]. De esta manera, a pesar de la impronta territorialista, se logra expandir el ámbito de aplicación de la ley.

4.8. Uruguay

En Uruguay, la Ley 18331 de Protección de Datos Personales, de 2008[68], es reglamentada por el Decreto 414/009[69], que en su artículo 3 establece dos criterios para determinar el ámbito espacial de aplicación de la ley, a saber:

1) que el tratamiento sea efectuado por un responsable "establecido en territorio uruguayo, siendo éste el lugar donde ejerza su actividad" y
2) que el responsable no establecido en territorio uruguayo "utilice en el tratamiento de datos medios situados en el país", excepto cuando lo haga exclusivamente con fines de tránsito y designe ante el órgano de control un representante[70] que tenga domicilio y residencia permanente en Uruguay.

Asimismo, otra ley posterior adicionó dos supuestos, con el objetivo de adaptar la normativa uruguaya al RGPD[71]. Se trata de la Ley 19670, de 2018[72], reglamentada por el Decreto 64/020[73]. En concreto, el artículo 37 de la Ley 19670 añadió la referencia al encargado en el criterio 1, referido en el párrafo precedente, y agregó dos nuevos criterios de aplicación de la ley nacional cuando el responsable o encargado no esté establecido en territorio uruguayo:

1) que las actividades de tratamiento estén "relacionadas con la oferta de bienes o servicios dirigidos a habitantes de la República o con el análisis de su comportamiento" y
2) que así lo dispongan normas de derecho internacional público o un contrato.

---

67 Vivian Velarde Wilson, entrevistada por Ana Karen de la Torre, "Panamá estrenará ley de protección de datos personales en 2021", *Lexlatin*, 1 de diciembre de 2020, https://bit.ly/3oW1rRc.

68 *IMPO, Centro de Información Oficial*, 18 de agosto de 2008, https://bit.ly/3uqeQSJ.

69 *IMPO, Centro de Información Oficial*, 15 de septiembre de 2009, https://bit.ly/3fT5fP5.

70 Según el segundo párrafo del artículo 3, la designación de dicho representante no impedirá la promoción de acciones legales contra el responsable.

71 Ana Brian Nourgreres, "El Sistema Uruguayo de Protección de Datos Personales y su posicionamiento global," *Revista Latinoamericana de Protección de Datos Personales*, n.° 5 (2018), IJ-DXLI-223, https://bit.ly/3fqtx3Z.

72 Ley de Aprobación de rendición de cuentas y Balance de ejecución presupuestal, Ejercicio 2017, *IMPO, Centro de Información Oficial*, 25 de octubre de 2018, https://bit.ly/3wunIYW.

73 *IMPO, Centro de Información Oficial*, 21 de febrero de 2020, https://bit.ly/3fsfF9u.

La comparación entre los criterios acogidos en los primeros tiempos de vigencia de la Ley 18331 para delimitar su ámbito territorial de aplicación y los previstos actualmente muestra una evolución positiva. Los supuestos contemplados se han modernizado, ajustándose un poco más al RGPD y quedando prácticamente idénticos a aquellos previstos en los Estándares.

CONCLUSIONES

El análisis normativo expuesto en el presente artículo permite concluir que la tendencia a la expansión del ámbito territorial de la legislación tuitiva en materia de protección de datos personales es una realidad en América Latina, y que en su desarrollo fue y sigue siendo importante el influjo de la regulación europea. En algunos casos se aprecia la influencia de la Directiva, mientras en otros prima la del RGPD o incluso la de ambos instrumentos.

Es un hecho que tanto la tendencia como la impronta de la UE continúan fortaleciéndose en Latinoamérica. Así lo demuestran el proyecto de ley de Argentina que delimita el ámbito territorial siguiendo el RGPD y la Ley Orgánica de Protección de Datos Personales de Ecuador que también recoge los criterios del RGPD. Sin embargo, considerando en conjunto la región, el impacto del modelo europeo en América Latina es matizado por el aún persistente territorialismo. Aquí vuelve a colación el ejemplo de Ecuador, pues a los criterios previstos en el RGPD se añaden dos, uno de los cuales es el del lugar del tratamiento en territorio ecuatoriano. En consecuencia, el influjo de la normativa europea no ha sido lo suficientemente vigoroso como para impedir que, actualmente, en América Latina tengan un fuerte peso criterios territoriales, en su momento rechazados por el RGPD.

Es por eso que en varios países siguen siendo importantes el lugar donde se efectúa el tratamiento, la localización de los datos personales y la ubicación de los medios empleados para tratarlos. De todos modos, si se toma como punto de partida cualquiera de estos tres criterios, es factible arribar a un resultado de extraterritorialidad y concluir en la aplicabilidad de la ley nacional a empresas responsables o encargadas del tratamiento de datos personales establecidas en el extranjero.

Ante el auge de empresas globales que tratan masivamente datos personales de individuos que se encuentran en Latinoamérica, es comprensible que los Estados de la región pretendan extender su abrazo protector fuera de sus límites jurisdiccionales. Entonces surge un gran desafío: el de la efectividad. Para enfrentarlo, es ineludible explorar nuevas avenidas de cooperación internacional.

BIBLIOGRAFÍA

1. Albornoz, María Mercedes. "El titular de datos personales, parte débil en tiempos de auge de la Inteligencia Artificial. ¿Cómo fortalecer su posición?" *Revista Ius* 15, n.° 48 (2021): 209-242, https://www.revistaius.com/index.php/ius/article/view/715/798
2. Azzi, Adèle. "The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation." *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 9, n.° 2 (2018): 126-137.

3. Brian Nourgreres, Ana. "El Sistema Uruguayo de Protección de datos personales y su posicionamiento global." *Revista Latinoamericana de Protección de Datos Personales*, n.° 5 (2018), IJ-DXLI-223, https://bit.ly/3fqtx3Z

4. "Carta de los Derechos Fundamentales de la Unión Europea, del 7 de diciembre de 2000," *Diario Oficial de la Unión Europea*, 7 de junio de 2016, https://bit.ly/3foFtmE

5. "Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal." Consejo de Europa del 28 de enero de 1981 *Serie de Tratados Europeos*, n.° 108. https://rm.coe.int/16806c1abd

6. "Data Protection Act No. 13 of 2011," *Tenth Parliament Republic of Trinidad and Tobago,* https://www.ttparliament.org/wp-content/uploads/2022/01/a2011-13.pdf

7. de la Chapelle, Bertrand y Paul Fehlinger. "Jurisdiction on the Internet: from Legal Arms Race to Transnational Cooperation." *Internet & Jurisdiction Paper* (2016): 1-28, https://bit.ly/3u8Yr4Z

8. "Decreto 414/009, Reglamentación de la Ley 18331, relativo a la protección de datos personales." *IMPO, Centro de Información Oficial*, 15 de septiembre de 2009, https://bit.ly/3fT5fP5

9. "Decreto 64/020. Reglamentación de los arts. 34 a 40 de la Ley 19670 y art. 12 de la Ley 18331, referente a la protección de datos personales." *IMPO, Centro de Información Oficial*, 21 de febrero de 2020, https://bit.ly/3fsfF9u

10. "Decreto Ejecutivo 37554-JP del 30 de octubre de 2012. Reglamento de la Ley n.º 8968." *Informática Jurídica*, 5 de marzo de 2013, https://bit.ly/3bPaCNT

11. "Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos." *Diario Oficial* n.º L 281 de 23 de noviembre de 1995, https://bit.ly/3g4PJjl

12. "Directrices 3/2018 relativas al ámbito territorial del RGPD (artículo 3), versión 2.1." Comité Europeo de Protección de Datos, 12 de noviembre de 2019, https://bit.ly/3yxGO2f

13. "Dictamen 8/2010 del 16 de diciembre de 2010, sobre el Derecho aplicable, emitido por el Grupo de Protección de Datos del Artículo 29, WP 179." *Informática Jurídica*, 16 de diciembre de 2020, https://bit.ly/3yqxtZS

14. "Estándares de Protección de Datos Personales para los Estados Iberoamericanos." *Red Iberoamericana de Protección de Datos*, 20 de junio de 2017, https://www.redipd.org/es/documentos/estandares-iberoamericanos

15. González Campos, Julio D. "Diversification, spécialisation, flexibilisation et matérialisation des règles de Droit international privé." *Recueil des cours de l'Académie de Droit International de La Haye* 287 (2000): 9-426

16. "Informe sobre la situación regional 2020." *Internet & Jurisdiction Policy Network*, https://bit.ly/3u8Br63

17. "Internet & Jurisdiction Global Status Report." *Internet & Jurisdiction Policy Network*, 2019, https://bit.ly/3fGKgPw

18. Kuner, Christopher. "Data Protection Law and International Jurisdiction on the Internet (Part 2)". *International Journal of Law and Information Technology* 18, n.° 3 (2010): 227-247.

19. ——. "Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law". *International Data Privacy Law* 5, n.° 4 (2015): 235-245.

20. "Legal Notice No. 2, of 2012, Republic of Trinidad y Tobago." https://bit.ly/34u3QsJ
21. "Ley 12965 de 23 de abril de 2014, establece principios, garantías, derechos y deberes para el uso de internet en Brasil." *Presidencia de la República*. https://bit.ly/3wIwLpn
22. "Ley 13709, Ley General de Protección de Datos Personales." *Presidencia de la República*, 15 de agosto de 2018, https://bit.ly/3bZ6ZVF
23. "Ley 172 que tiene por objeto la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados." República Dominicana, *Gaceta Oficial*, 15 de diciembre de 2013, https://bit.ly/3fNVVMb
24. "Ley 18331 de Protección de Datos Personales." *IMPO, Centro de Información Oficial*, 18 de agosto de 2008, https://bit.ly/3uqeQSJ
25. "Ley 19628 sobre Protección de la Vida Privada." Ministerio Secretaría General de la Presidencia. 28 de agosto de 1999. *Biblioteca del Congreso Nacional de Chile*, http://bcn.cl/1uv2v
26. "Ley 19670, Aprobación de rendición de cuentas y balance de ejecución presupuestal, Ejercicio 2017." *IMPO, Centro de Información Oficial*, 25 de octubre de 2018, https://bit.ly/3wunIYW
27. "Ley 25.326, Protección de los Datos Personales." Argentina, *Ministerio de Justicia y Derechos Humanos, Presidencia de la Nación*, 2 de noviembre de 2000, https://bit.ly/2QXaWmx
28. "Ley 29733, Ley de Protección de Datos Personales." *Sistema Peruano de Información Jurídica*, 3 de julio de 2011, https://bit.ly/2SBl4BN
29. "Ley 6534 de Protección de Datos Personales Crediticios." *Gaceta Oficial de la República del Paraguay*, 28 de octubre de 2020, http://www.gacetaoficial.gov.py/index/getDocumento/65863
30. "Ley 787 de Protección de Datos Personales." *La Gaceta. Diario Oficial*, 29 de marzo de 2012, https://bit.ly/3bPTkAd
31. "Ley 81 sobre Protección de Datos Personales." *República de Panamá, Asamblea Nacional*, 29 de marzo de 2019, https://bit.ly/34omPVS
32. "Ley 8968 sobre Protección de la Persona frente al Tratamiento de sus Datos Personales." *Sistema Costarricense de Información Jurídica*, 5 de septiembre de 2011, https://bit.ly/3oIJyp1
33. "Ley Estatutaria 1581 de 2012 (octubre 17), por la cual se dictan disposiciones generales para la protección de datos personales." *Secretaría del Senado*, 18 de octubre de 2012, https://bit.ly/3hWj2a8
34. "Ley Federal de Protección de Datos Personales en Posesión de los Particulares." *Cámara de Diputados del H. Congreso de la Unión*, 5 de julio de 2010, https://bit.ly/2SytrxY
35. "Ley Orgánica de Protección de Datos Personales." *Registro Oficial*, órgano de la República del Ecuador, 26 de mayo de 2021, https://bit.ly/3wxPDqO
36. Miguel Asensio, Pedro Alberto de. "Competencia y derecho aplicable en el Reglamento General sobre protección de datos de la Unión Europea." *Revista Española de Derecho Internacional* 69, n.° 1 (2017): 75-108.
37. Moura Vicente, Dário y Sofia de Vasconcelos Casimiro. "Data Protection in the Internet: General Report." En *Data Protection in the Internet*, edited by Dário Moura Vicente and Sofia de Vasconcelos Casimiro. Cham: Springer, 2020.

38. Parentoni, Leonardo y Henrique Cunba Souza Lima. "Proteção de Dados Pessoais no Brasil: Antinomias Internas e Aspectos Internacionais." En *Direito & Internet IV. Sistema de Proteção de Dados Pessoais*, coordinado por Newton de Lucca, Adalberto Simão Filho, Cintia Rosa Pereira de Lima y Renata Mota Maciel, 483-511. San Pablo: Quartier Latin, 2019.

39. Pereznieto Castro, Leonel. "La tradition territorialiste en droit international privé dans les pays d'Amérique Latine." En *Recueil des cours de l'Académie de Droit International de La Haye,* 1985, 271-400. Dordrecht: Martinus Nijhoff Publishers, 1986.

40. "Principios Actualizados del Comité Jurídico Interamericano sobre la Privacidad y la Protección de Datos Personales, con anotaciones." *Organización de Estados Americanos*, 9 de abril de 2021, https://bit.ly/3i3iIXn

41. "Proyecto de ley 2986-S-20020". *Senado Argentina*, https://www.senado.gob.ar/parlamentario/comisiones/verExp/2986.20/S/PL

42. "Proyecto de ley 6234-D-2020, Ley de protección de Datos Personales." *Diputados Argentina*, https://bit.ly/3uttkRL

43. "Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo del 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." *Diario Oficial de la Unión Europea*, 4 de mayo de 2016, https://bit.ly/3fs05ui

44. "Reglamento de la Ley 29733, Ley de Protección de Datos Personales, Decreto Supremo 003-2013-JUS." *El Peruano*, 22 de marzo de 2013, https://bit.ly/3vEoiTG

45. "Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares." *Cámara de Diputados del H. Congreso de la Unión,* 21 de diciembre de 2011, https://bit.ly/34omnHa

46. Remolina, Nelson. *Recolección internacional de datos personales: un reto del mundo post-internet*. Madrid: Agencia Española de Protección de Datos - Agencia Estatal Boletín Oficial del Estado, 2015.

47. "Resolución 15342, 28 de marzo de 2022, por la cual se resuelve un recurso de apelación." *República de Colombia. Ministerio de Comercio, Industria y Turismo. Superintendencia de Industria y Comercio*, https://www.sic.gov.co/sites/default/files/documentos/042022/Resolucion-15342-de-28-marzo-de-2022_WhatsApp-LLC.pdf

48. "Resolución 12192, 1 de abril de 2020." *República de Colombia. Ministerio de Comercio, Industria y Turismo. Superintendencia de Industria y Comercio,* https://www.sic.gov.co/sites/default/files/files/2020/Res%2012192%2001IV2020%20SIC%20Facebook%20Inc.pdf

49. "Resolución 2389, 28 de enero de 2022, por la cual se resuelve una solicitud de revocatoria directa." *República de Colombia. Ministerio de Comercio, Industria y Turismo. Superintendencia de Industria y Comercio* https://www.sic.gov.co/sites/default/files/documentos/022022/Resolucion2389-de-28-de-enero-de-2022_GoogleLLC.pdf

50. Ryngaert, Cedric and Mistale Taylor. "The GDPR as *Global* Data Protection Regulation?" *AJIL Unbound* 114, (2020): 5-9, https://bit.ly/3ykAv1X

51. Scott, Joanne. "Extraterritoriality and Territorial Extension in EU Law". *American Journal of Comparative Law* 62, n.° 1 (2014): 87-125.

52. Svantesson, Dan Jerker B. "The Extraterritoriality of EU Data Privacy Law - Its Theoretical Justification and Its Practical Effect on U.S. Businesses". *Stanford Journal of International Law* 50, n.° 1 (2014): 53-102.

53. "Texto refundido, coordinado y sistematizado del código civil; de la Ley n.º 4.808, sobre registro civil; de la Ley n.º 17.344, que autoriza cambio de nombres y apellidos; de la Ley n.º 16.618, Ley de Menores; de la Ley nº 14.908, sobre abandono de familia y pago de pensiones alimenticias; y de la Ley n.º 16.271, de impuesto a las herencias, asignaciones y donaciones." 16 de mayo de 2000. *Biblioteca del Congreso Nacional de Chile,* http://bcn.cl/1uu74

54. Thon, Marian. "Transnationaler Datenschutz: Das Internationale Datenprivatrecht der DS-GVO". *Rabels Zeitschrift für ausländisches und internationales Privatrecht* 84, n.° 1 (2020): 24-61.

55. Velarde Wilson, Vivian, entrevistada por Ana Karen de la Torre. "Panamá estrenará ley de protección de datos personales en 2021." *Lexlatin*, 1 de diciembre de 2020, https://bit.ly/3oW1rRc