

La senda del efecto Bruselas en la DMA en Latinoamérica

Alba Ribera Martínez*

Universidad Carlos III (España)

Recibido: 28 de octubre del 2022 | Aceptado: 26 de abril del 2023

Cómo citar: Ribera Martínez, Alba. “La senda del efecto Bruselas en la DMA en Latinoamérica”. *Latin American Law Review* n.º 11 (2023): 93-110, doi <https://doi.org/10.29263/lar11.2023.05>

Resumen

En este artículo se compara el impacto de la Ley de Mercados Digitales (DMA) a partir de los efectos inadvertidos que el Reglamento General de Protección de Datos (RGPD) proyectó en la normativa latinoamericana. Primero, se analiza de qué forma se articula el efecto Bruselas de forma generalizada. Luego, se consideran los efectos extraterritoriales causados por la normativa europea en materia de protección de datos en Latinoamérica tanto por vía normativa como jurisprudencial. Finalmente, se señalan los futuros efectos de la DMA desde la perspectiva de la designación de los llamados guardianes de acceso, la imposición de obligaciones y la duplicación de procedimientos sancionadores, como resultado de los efectos reflejos causados por el efecto Bruselas.

Palabras clave

Ley de Mercados Digitales, protección de datos personales, efecto Bruselas, plataformas digitales, usuarios latinoamericanos

Tracing the DMA's Brussels Effect on Latin America

Abstract

Stemming from the experience regarding the effects of the General Data Protection Regulation (GDPR) in Latin America, the paper captures this same phenomenon applied to the Digital Markets Act's (DMA) future entry into force. First, the paper will analyse the Brussels effect in its broadest terms. Then, the paper considers the extraterritorial effects of the Union's standards in terms of protection of personal data in Latin America, both from a normative and case-law perspective. Finally,

* Doctoranda en Derecho de la competencia, Universidad Carlos III de Madrid (Madrid, España); docente en Universidad Villanueva (Madrid, España). ORCID: 0000-0002-9152-0030. ✉ riberamartinezalba@gmail.com

the paper takes into account the future impact of the DMA in Latin America in light of the designation of gatekeepers, the force of the DMA's prohibitions and obligations as well as the possible duplication of proceedings at the enforcement level.

Keywords

Digital Markets Act, Protection of Personal Data, Brussels Effect, Digital Platforms, Latin American Users

INTRODUCCIÓN

En octubre de 2022, la Digital Markets Act (Ley de Mercados Digitales –DMA) se publicó oficialmente, y sus disposiciones entraron en vigor en noviembre de ese mismo año, a pesar de que sus obligaciones no comenzarán a aplicarse hasta marzo de 2024¹. La DMA aborda el problema de la disputabilidad y la equidad en los mercados digitales². Es decir, al haberse detectado varios fallos de mercado en sede de la aplicación pública del Derecho de la competencia, la Comisión Europea y el Parlamento Europeo optaron por promulgar unas nuevas normas que se apliquen solamente a determinados operadores digitales que han contribuido enormemente a generar estos desequilibrios en el mercado.

La DMA introduce tres grandes ideas en el panorama de las plataformas digitales. En primer lugar, designa a determinados operadores económicos como guardianes de acceso en relación con los servicios que prestan³. Estos son los únicos que se verán limitados en su modelo de negocio a raíz de la promulgación de la DMA. Una vez se haya completado el proceso de designación, a esos mismos guardianes de acceso se les impondrán una serie de obligaciones y prohibiciones en virtud de los artículos 5 a 7. Finalmente, la Comisión Europea es la encargada de supervisar el cumplimiento de estas obligaciones, a través de la posibilidad de incoar procedimientos en caso de que se produzcan incumplimientos que pueden culminar en sanciones de hasta un diez por ciento de su volumen de negocios⁴.

1 European Parliament and Council, *Regulation (EU) of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act)*. 2022/1925, Brussels. https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ%3AL%3A2022%3A265%3ATOC&uri=uriserv%3AOJ.L_.2022.265.01.0001.01.ENG (accessed October 12, 2022). A pesar de que la traducción oficial señala que la DMA se interpreta como Ley de Mercados Digitales, realmente adopta la forma de un reglamento comunitario, que es directamente aplicable en cada Estado Miembro sin requerir de un previo desarrollo legislativo en el ámbito nacional.

2 De acuerdo con el Considerando 32, la disputabilidad “debe estar relacionada con la capacidad de las empresas para superar de forma efectiva los obstáculos a la entrada y la expansión, y competir con el guardián de acceso sobre la base de la calidad intrínseca de sus productos y servicios” y de acuerdo con el Considerando 33, la falta de equidad “debe estar relacionada con un desequilibrio entre los derechos y las obligaciones de los usuarios profesionales en el que el guardián de acceso obtenga una ventaja desproporcionada”.

3 European Parliament and Council. *Digital Markets Act*, Article 3. Una empresa es designada como guardián de acceso si “a) tiene una gran influencia en el mercado interior; b) presta un servicio básico de plataforma que es una puerta de acceso importante para que los usuarios profesionales lleguen a los usuarios finales, y c) tiene una posición afianzada y duradera, por lo que respecta a sus operaciones, o es previsible que alcance dicha posición en un futuro próximo”.

4 European Parliament and Council. *Digital Markets Act*, Articles 18 and 30(1).

En este nuevo marco normativo, la Unión Europea⁵ prevé restaurar las condiciones competitivas de determinados mercados digitales dentro del mercado interior. Sin embargo, este cambio normativo va a suponer una verdadera revolución ante la forma de operar de estas mismas plataformas digitales a escala mundial, a raíz del término acuñado por Anu Bradford como «efecto Bruselas»⁶.

Desde principios de siglo, en algunos de los sectores más destacados de la regulación mundial como la normativa de protección de datos personales, la normativa alimentaria o la normativa de competencia, estamos siendo espectadores de las consecuencias de este efecto Bruselas⁷. Según Bradford, dicho efecto es aquel en virtud del cual las normas regulatorias europeas, que tienen, en principio, únicamente alcance regional, pasan a ser consideradas el estándar global aplicable en el resto de las jurisdicciones del mundo. Como precondition de su ejercicio, el mercado europeo debe ejercer una especial *vis atractiva* respecto del resto de mercados mundiales para poder ejercer su poder⁸. Para que se produzca dicho efecto, deben concurrir cuatro características fundamentales: i) la capacidad regulatoria de la propia Unión; ii) la voluntad política de la Unión de imponer unos estándares más restrictivos en determinados sectores; iii) la inelasticidad (entendida en un sentido amplio) de las actividades y sectores económicos a los que se sujeta a esa regulación; y iv) la indivisibilidad del ejercicio de esas mismas actividades económicas en la Unión, respecto de su ejercicio en el resto de las jurisdicciones del mundo⁹. En concreto, la inelasticidad de las actividades económicas se refiere a la incapacidad de los operadores económicos situados en la Unión de dejar de operar en este territorio, por las graves consecuencias económicas que puede provocar dicha decisión.

A partir de las características que se han expuesto en relación con el efecto Bruselas, en el artículo se analiza de qué forma se ha proyectado este efecto en sede latinoamericana, a partir de las normas aprobadas a nivel comunitario en materia de protección de datos personales. Adicionalmente, se considera tanto el impacto de la inicial y novedosa Directiva de 1995¹⁰, como del Reglamento General de Protección de Datos (RGPD) que vendría a derogarla en 2016 y que entró en vigor en 2018¹¹. Además de señalar los cambios normativos que se han producido en Latinoamérica en esta materia, se observarán dos hechos fundamentales que han tenido lugar y que han irradiado sus efectos por vía jurisprudencial: el nacimiento del derecho

5 A lo largo del texto se utilizarán indistintamente los términos UE y Unión para referirse a la Unión Europea.

6 Bradford, *The Brussels Effect*; Ibáñez Colomo, “The Draft Digital Markets Act”; Petit, “The Proposed Digital Markets Act”.

7 Bradford, *The Brussels Effect*; Ibáñez Colomo, “The Draft Digital Markets Act”; Petit, “The Proposed Digital Markets Act”.

8 Bradford, “The Brussels Effect” *Northwestern University Law Review* 107, no. 1 (2012): 1-64.

9 Bradford, *The Brussels Effect*, 25-65.

10 European Parliament and the Council. *Directive on the protection of individuals with regard to the processing of personal data on the free movement of such data*. 95/46/EC, Brussels. <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A31995L0046> (accessed October 11, 2022).

11 European Parliament and the Council. *Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC* (General Data Protection Regulation). (EU) 2016/679, Brussels. <http://data.europa.eu/eli/reg/2016/679/oj> (accessed October 9, 2022).

al olvido¹² (el derecho del interesado a oponerse a la indexación de sus datos personales por un motor de búsqueda cuando su difusión pueda causarle un perjuicio) en Latinoamérica y la ampliación del régimen de protección relativo a las transferencias internacionales de datos personales¹³ (aquellas situaciones en las que se transfieren datos fuera de la Unión a terceros Estados y que normalmente vienen regidas por una decisión de adecuación pactada con la Comisión Europea).

Por lo que respecta a las conclusiones de la sección primera del artículo, el aparte final está dedicado a la traslación de los componentes que se han analizado transversalmente en materia de protección de datos personales al caso de la DMA. En concreto, se detiene en el procedimiento de designación de los guardianes de acceso y su potencial afectación a los operadores económicos latinoamericanos. Posteriormente, se analiza la forma en la que la DMA transformará los modelos de negocio existentes en las plataformas digitales que operan en Latinoamérica, imponiéndoles un costo y una carga regulatoria que no está necesariamente legitimada en el ejercicio del poder legislativo nacional. Se concluye indicando el espacio abierto para la aplicación pública del Derecho de la competencia por parte de las autoridades nacionales de competencia latinoamericanas, una vez se hayan materializado los efectos de la DMA.

El epígrafe A está dedicado a la explicación del efecto Bruselas y a la exposición del impacto de la normativa en materia de protección de datos personales en Latinoamérica. La sección segunda (epígrafe B) se adentra en las implicaciones prácticas que la DMA proyectará sobre el ámbito latinoamericano.

Por su parte, la sección segunda considera directamente el efecto Bruselas en lo relativo a la aplicación de sus disposiciones. En este sentido, el epígrafe A se ocupa de destacar dichos efectos desde la perspectiva subjetiva, es decir, los operadores económicos que se verán afectados por la regulación, que también están presentes en el mercado latinoamericano. El epígrafe B establece las divergencias regulatorias que se acusarán por estos mismos operadores económicos desde la perspectiva objetiva. Por su virtud, se analizarán las disposiciones aplicables a los guardianes de acceso en sus modelos de negocio así como las posibles consecuencias que se pueden producir a raíz de su incumplimiento (epígrafe C).

12 *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, Case C-131/12, ECLI:EU:C:2014:317 (Court of Justice of the European Union, Grand Chamber. May 13, 2014). <https://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=533401>; *Google LLC v Commission nationale de l'informatique et des libertés (CNIL)*, Case C-507/17, ECLI:EU:C:2019:772 (Court of Justice of the European Union, Grand Chamber. September 24, 2019). <https://curia.europa.eu/juris/document/document.jsf?jsessionid=9E06FCDDC86A384492677F5FE997C753?text=&docid=218105&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=532646>.

13 *Maximilian Schrems v Data Protection Commissioner*, Case C-362/14, ECLI:EU:C:2015:650 (Court of Justice of the European Union, Grand Chamber. October 6, 2015). <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62014CJ0362>; *Maximilian Schrems v Facebook Ireland Limited*, Case C-498/16, ECLI:EU:C:2018:37 (Court of Justice of the European Union, Third Chamber. January 25, 2018). <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62016CJ0498>; *Data Protection Commissioner v Facebook Ireland Limited and Maximilian Schrems*, Case 311/18, ECLI:EU:C:2020:559 (Court of Justice of the European Union, Grand Chamber. July 16, 2020). <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62018CJ0311>.

EL IMPACTO DE LA REGULACIÓN EUROPEA EN LOS ESTÁNDARES DE PROTECCIÓN GLOBALES

Durante los últimos veinte años la Unión Europea ha fijado los estándares de protección en determinados sectores, gracias al efecto Bruselas. En virtud de este fenómeno, el ámbito con más atractivo por lo que se refiere al poder adquisitivo de los consumidores, es capaz de fijar los estándares que rigen a nivel mundial los intercambios de productos y servicios. Es evidente que dicho efecto Bruselas podría haberse producido en cualquier otra parte del mundo. Podríamos tener un efecto Washington o un efecto Pekín, pero la Unión Europea ha sido capaz de erigirse como el poder hegemónico mundial en lo que se refiere a la promulgación de estándares normativos, dado que los consumidores europeos son quienes gozan de un mayor nivel de gasto a nivel mundial¹⁴. El resto de las jurisdicciones, por tanto, no tienen como obviar completamente al consumidor europeo, ya que una gran parte de sus exportaciones se dirigen precisamente a ese territorio¹⁵.

Este es el motivo por el que Bradford, dentro de su marco teórico, fija que la *vis atractiva* del mercado del que se trate, en este caso el mercado de la Unión es una precondition para que se pueda producir el efecto Bruselas, sin perjuicio de que solamente afectará a aquellos sectores que cumplan con dos características determinadas, que se señalan a continuación¹⁶.

A. El efecto Bruselas

En el marco de esta situación, la Unión podría haber optado por fijar sus estándares normativos en coherencia con el resto de las jurisdicciones mundiales, con el fin de promulgar y facilitar el comercio entre distintos países. Sin embargo, la decisión y la voluntad política a lo largo de la evolución de la Unión ha seguido otra senda completamente distinta: la del reforzamiento del mercado interior de la UE a través de la fijación de unos estándares más exigentes de protección para los consumidores. De modo contrario a la política por la que han optado otros países del mundo para aliviar la carga regulatoria sobre su comercio, la Unión Europea se ha decantado claramente por la promulgación de una serie de normativas de carácter intervencionista en distintos sectores¹⁷.

Partiendo del atractivo del mercado europeo, la Unión ha implementado una normativa que protege en mayor medida a sus consumidores y, por extensión, a los del resto de jurisdicciones mundiales. El tejido empresarial mundial tiende a adoptar los estándares normativos europeos en aquellos sectores que se caracterizan por dos características concretas.

Primera: estos efectos solamente se producen en aquellos sectores inelásticos en un sentido amplio. Un sector es inelástico a estos efectos cuando tiene una escasa capacidad para deslocalizar sus activos empresariales del territorio de la Unión Europea, con el fin de evitar

14 Google, "European Union Consumer Spending"; Google, "United States Indicators"; Google, "China Indicators".

15 Spar y Yoffie, "A Race to the Bottom?".

16 Bradford, *The Brussels Effect*, 26-30; Bach y Newman, "The European regulatory state"; Damro, "Market power Europe".

17 Bradford, *The Brussels Effect*, 30-48; Kogan, "Exporting Europe's Protectionism", 92.

que se le aplique su misma normativa. Por ejemplo, en el sector digital se aplicarán directa y automáticamente las exigencias de la normativa europea cuando nos encontremos ante supuestos de hecho en los que concurra, al menos, un consumidor europeo. En este tipo de situaciones, es completamente irrelevante en qué lugar se establezca la empresa. El sector es inelástico porque la posibilidad de evitar la aplicación de la norma europea a través de la deslocalización es baja¹⁸.

Segunda: el efecto Bruselas se produce en aquellos sectores en los que los costes de aplicar el estándar más limitativo son menores a los costes de aplicar los distintos estándares normativos, dependiendo de la jurisdicción en la que opere la empresa. Es decir, en algunos sectores, como el digital, puede ser más rentable para la empresa unificar la normativa que otorga una mayor protección y aplicarla al conjunto de sus consumidores, para que así absorba el coste de cumplimiento del resto de los estándares fijados en los regímenes jurídicos del resto de las jurisdicciones en las que opere¹⁹.

Estas características generales son las que conducen a la definición de unos estándares de protección fácticos y jurídicos comunes. En el primer caso, el estándar europeo se aplica y adopta en esa jurisdicción por vía de la práctica empresarial. En el segundo caso, una vez que el fenómeno ha arraigado en las decisiones de los operadores económicos, los poderes legislativos de otras jurisdicciones distintas a la Unión promulgan sus propias normas incorporando esos mismos estándares e incluso unos estándares más elevados a sus propios regímenes jurídicos.

B. La protección de los datos personales en Latinoamérica

La protección de los datos personales, como materia, se ajusta a las características generales que hemos observado en relación con el efecto Bruselas²⁰. Desde sus orígenes en la normativa europea, el nivel de protección que se confiere está orientado a asegurar el establecimiento y funcionamiento del mercado interior, a través de la libre circulación de los datos personales de un Estado miembro a otro y de la protección de los derechos fundamentales de las personas.

Desde 1995, la Unión Europea lidera la integración de la normativa relativa al tratamiento y a los intercambios transfronterizos de datos personales en el mundo, al ser la primera jurisdicción en fijar un régimen de protección respecto del usuario europeo en torno a su privacidad²¹, sin perjuicio de que en otros foros internacionales se desarrollaron los estándares que regirían la posterior normativa comunitaria en materia de protección de datos personales. La Unión se erige, en este momento, como la jurisdicción con el estándar de protección más elevado respecto a la protección de datos personales.

18 Bradford, *The Brussels Effect*, 48-53.

19 Bradford, *The Brussels Effect*, 53-62.

20 Bradford, *The Brussels Effect*, 132-155; Bach y Newman, "The European regulatory state", 830; Shaffer, "Globalization and Social Protection", 7-21.

21 Lam, "Unsafe Harbor: The European Union's Demand", 1; Bergkamp, "EU Data Protection Policy: The Privacy Fallacy", 32-33; Martínez, "From *Habeas Data* Action to *Omnibus* Data Protection".

Por contraposición, podríamos pensar que el resto de las jurisdicciones del mundo no habían prestado ninguna atención en cuanto a regular dicha materia. Sin embargo, si nos fijamos en el ámbito latinoamericano, comprobamos que no es así. A pesar de que en ese momento (1995) no se habían promulgado normas nacionales comprehensivas relativas al derecho a la protección de los datos personales, los textos constitucionales de los distintos Estados latinoamericanos ya contemplaban su protección como un derecho inherente a la propia condición humana del individuo²², por derivación de los estándares promulgados a principios de los años 1980 en los foros de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) y el Consejo de Europa²³. Incluso algunos países latinoamericanos contemplaron explícitamente un procedimiento de carácter constitucional de *habeas data* ya en ese momento²⁴. Este procedimiento confería un derecho accionable, aunque *ex post*, en favor del individuo que podría reclamar ante los tribunales para instar la protección de sus datos personales en determinados ámbitos²⁵.

Sin embargo, la Directiva de 1995 alteró esta senda que seguía la protección de los datos personales en Latinoamérica, apegada al control judicial y al caso concreto, en favor de un régimen omnicompreensivo de la protección de los datos personales como un derecho individualizado²⁶. En el periodo desde la aprobación de la Directiva hasta la entrada en vigor del RGPD, ocho países latinoamericanos aprobaron sus leyes generales de protección de datos personales inspirándose en el modelo planteado por la entonces aplicable Ley Orgánica de Protección de Datos de Carácter Personal española²⁷: Argentina (2000)²⁸, Uruguay (2008)²⁹,

22 Brazilian Constitution. art. 5, § LXVII-LXXVII; Guatemalan Constitution. art. 31; Nicaraguan Constitution. art. 26; Colombian Constitution. art. 15; Paraguayan Constitution. art. 135; Peruvian Constitution, art. 200; Argentinian Constitution. art. 43 § III; Ecuadorian Constitution. art. 30; Venezuelan Constitution. art. 27-28.

23 OECD. "Guidelines on the Protection of Privacy".

24 Brazilian Constitution. art. 5, § LXXII; Congreso de la Nación Paraguaya, Ley que reglamenta la información de carácter privado (*Ley n.º 1.682*), Asunción, 2001, <https://www.bacn.gov.py/leyes-paraguayas/1760/ley-n-1682-reglamenta-la-informacion-de-caracter-privado>; Congreso Constituyente Democrático, Ley que modifica la Constitución Política del Estado, en lo referido a las Garantías Constitucionales. Reforma Constitucional del artículo 200 relativo al Habeas Data (*Ley 26.470*), Lima, 1995, <https://www.informatica-juridica.com/anexos/ley-26-470-de-31-de-mayo-de-1995-que-modifica-la-constitucion-politica-del-estado-en-lo-referido-a-las-garantias-constitucionales-reforma-constitucional-del-articulo-200-relativo-al-habeas-data-promul/>; Congreso Nacional del Ecuador, Ley del Control Constitucional (*R-22-058*), San Francisco de Quito, 1997, <https://docs.ecuador.justia.com/nacionales/leyes/ley-de-control-constitucional.pdf>, arts. 34-35; Congreso Nacional de Chile, Ley sobre protección de la vida privada (*Ley 19628*), Santiago, 1999, https://cms-dgd-prod.s3-us-west-2.amazonaws.com/uploads/pdf/LEY-19628_28-AGO-1999.pdf.

25 Brian Nougères, "Data Protection and Enforcement in Latin America and in Uruguay", 146-149; Puccinelli, "Evolución histórica y análisis", 477-487.

26 Brian Nougères, "Chapter 7", 148-149.

27 Cortes Generales, *Ley Orgánica de Protección de Datos de Carácter Personal (LO 15/1999)*, Madrid, 1999, <https://www.boe.es/eli/es/lo/1999/12/13/15>.

28 Honorable Congreso de la Nación Argentina, *Habeas Data (Ley 25.326)*, Buenos Aires, 2000, <https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790/texto>.

29 Asamblea General del Poder Legislativo de la República Oriental del Uruguay, *Ley de protección de datos personales (Ley n.º 18331)*, Montevideo, 2008, <https://www.imo.com.uy/bases/leyes/18331-2008>.

México (2010)³⁰, Costa Rica (2011)³¹, Nicaragua (2011)³², Perú (2011)³³, Colombia (2012)³⁴ y República Dominicana (2013)³⁵.

Tanto la Directiva de 1995 como el posterior RGPD contemplan la perspectiva extraterritorial de la normativa: de forma más atenuada en la primera y más pronunciada en la segunda³⁶. Por lo que se refiere a la perspectiva latinoamericana, el cambio normativo se produjo en el ínterin entre ambas regulaciones, sin perjuicio de que el resto de los avances en la normativa por vía jurisprudencial también adelanten los riesgos inherentes al efecto Bruselas.

En esta materia, la evolución y el nacimiento del derecho al olvido, así como la regulación relativa a las transferencias internacionales de datos personales, evidencian que el conjunto normativo europeo tiene un carácter flexible, puesto que los criterios interpretativos de sus normas se adaptan fácilmente en un sentido u otro (de expansión o de restricción) gracias a la actuación del Tribunal de Justicia, por vía de la cuestión prejudicial prevista en el artículo 267 del Tratado de Funcionamiento de la Unión Europea en la interpretación del RGPD, así como de la intervención del Comité Europeo de Protección de Datos.

-
- 30 Cámara de Diputados del Honorable Congreso de la Unión, *Ley Federal de protección de datos personales en posesión de los particulares (Ley DOF 05-07-2010)*, Ciudad de México, 2010, <http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf>.
 - 31 Asamblea Legislativa de la República de Costa Rica, *Ley de protección de la persona frente al tratamiento de sus datos personales (Ley n° 8968)*, San José, 2011, <https://www.tse.go.cr/pdf/normativa/leydeproteccionde lapersona.pdf>.
 - 32 Asamblea Nacional de la República de Nicaragua, *Ley de Protección de Datos Personales (Ley n.º 787)*, Managua, 2011, <https://www.informatica-juridica.com/anexos/ley-no-787-de-21-de-marzo-de-2012-de-proteccion-de-datos-personales-nicaragua-nbsp-la-gaceta-diario-oficial-no-61-de-29-de-marzo-de-2012/>.
 - 33 Congreso de la República de Perú, *Ley de Protección de Datos Personales (Ley N.º 29733)*, Perú, 2011, <https://cdn.www.gob.pe/uploads/document/file/272360/Ley%20N%C2%BA%2029733.pdf.pdf?v=1618338779>, Accessed October 20, 2022.
 - 34 Congreso de Colombia, *Ley Estatutaria por la cual se dictan disposiciones generales para la protección de los datos personales (Ley n° 1581)*, Bogotá, 2012, <https://www.informatica-juridica.com/anexos/ley-estatutaria-1581-de-17-de-octubre-de-2012-por-la-cual-se-dictan-disposiciones-generales-para-la-proteccion-de-los-datos-personales-diario-oficial-48587-de-octubre-18-de-2012/>. En el ámbito colombiano se particulariza dicha protección mediante la Ley 1266 de 2008, Ley estudiada por la Corte Constitucional mediante Sentencia C-1011 de 2008 por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial de servicios y la proveniente de terceros países y se dictan otras disposiciones, Bogotá, 2008, <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488>.
 - 35 Congreso Nacional de la República Dominicana, *Ley 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 (Ley No. 172-13)*, Santo Domingo de Guzmán, 2013, https://indotel.gob.do/media/6200/ley_172_13.pdf; María de Lourdes Zamudio Salinas, “El marco normativo latinoamericano y la Ley de protección de datos personal del Perú” *Revista Internacional de Protección de Datos Personales* No. 1 (2012): 9, https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/ok3_Ma.-de-Lourdes-Zamudio_FINAL.pdf; Brian Nougères, “Chapter 7”, 153-155.
 - 36 European Parliament and the Council, *Directive on the protection of individuals*, Recital 19; European Parliament and the Council, *General Data Protection Regulation*, Recitals 22-25. Desde la perspectiva normativa, la Directiva de 1995 y el RGPD difieren en cuanto a forma, ya que la primera exigió que los Estados Miembros transpusieran su contenido al ámbito nacional, mientras que el RGPD, dada su naturaleza de Reglamento, devino directamente aplicable a los Estados Miembros una vez entró en vigor en 2018.

En el caso del derecho al olvido, este fenómeno se evidencia primero a través del nacimiento de un derecho, de mano de la interpretación del Tribunal de Justicia de la Unión Europea (TJUE), que no estaba contenido en la normativa en vigor (la Directiva de 1995), y que posteriormente se regularía por vía del art. 17 del RGPD. El TJUE, en el asunto *Google contra AEPD y Mario Costeja González*³⁷, delimita el alcance del derecho de forma general. La sentencia apela directamente al carácter extraterritorial de la normativa europea de protección de datos, al señalar que a pesar de que el motor de búsqueda (en este caso, Google) sea gestionado por una empresa de un tercer Estado, las actividades relativas a su funcionamiento y a su actividad comercial no se pueden ver sustraídas de las garantías y obligaciones establecidas por la Unión Europea en esta materia³⁸. Sin embargo, posteriormente a través del asunto *Google contra CNIL*, el TJUE circunscribe la proyección de los efectos del derecho al olvido al territorio de la Unión³⁹, sin perjuicio de que en el ínterin se había avanzado ya extraterritorialmente en cuanto a su desarrollo⁴⁰.

En Latinoamérica, hasta cinco jurisdicciones distintas introdujeron un derecho similar, así: por vía jurisprudencial (Argentina⁴¹, Chile⁴² y parcialmente en Colombia⁴³), por vía legislativa (Nicaragua⁴⁴) y por vía de sus propias autoridades en materia de protección de datos (México⁴⁵)⁴⁶. El efecto del primer pronunciamiento del TJUE ya se había manifestado en las distintas jurisdicciones latinoamericanas, y afectó a las extensiones y dominios nacionales

37 *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, Case C-131/12, párr. 88.

38 *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, Case C-131/12, párr. 58.

39 *Google LLC v Commission nationale de l'informatique et des libertés (CNIL)*, Case C-507/17, paras 59-64. En línea con las recomendaciones del Article 29 Data Protection Working Party, *Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12*. 14/EN WP 225, Brussels. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf.

40 Frosio, "The Right to be Forgotten", 330.

41 *Rodríguez María Belén c/ Google Inc. s/ daños y perjuicios*, Fallos: 337:1174 (Corte Suprema de Justicia de la Nación, October 28, 2014). <https://sjconsulta.csjn.gov.ar/sjconsulta/documentos/verDocumentoByIdLinksJP.html?idDocumento=7162581&cache=1665730605006>; Carter, "Argentina's Right to be Forgotten", 23.

42 Luiz Fernando Marrey Moncau, "Causa n.º 22243/2015 (Apelación). Resolución n.º 36142 of Corte Suprema", *Wilmap*, January 21, 2016, <https://wilmap.stanford.edu/entries/causa-no-222432015-apelacion-resolucion-no-36142-corte-suprema>.

43 *Acción de tutela instaurada por Gloria contra la Casa Editorial El Tiempo*, Sentencia T-277/15, Expte. T-4296509 (Corte Constitucional, Sala Primera de Revisión, May 12, 2015). <https://www.corteconstitucional.gov.co/Relatoria/2015/T-277-15.htm>; *Acción de tutela instaurada por Guillermo Martínez Trujillo contra Google Colombia Ltda. y la Casa Editorial El Tiempo*, Sentencia T-040/13, Expte. T-3.623.589 (Corte Constitucional, Sala Séptima de Revisión de tutelas, January 28, 2015). <https://www.corteconstitucional.gov.co/Relatoria/2013/T-040-13.htm>.

44 Asamblea Nacional, *Ley de Protección de Datos Personales*, 787, Managua, 2012. <http://legislacion.asamblea.gob.ni/normaweb.nsf/9e314815a08d4a6206257265005d21f9/e5d37e9b4827fc06062579ed0076ce1d> (accessed October 13, 2022), artículo 10.

45 *Caso IFAI Google México*, PPD.0094/14 (Instituto Federal de Acceso a la Información y Protección de Datos, January 26, 2015). <http://inicio.ifai.org.mx/pdf/resoluciones/2014/PPD%2094.pdf>.

46 En la jurisdicción brasileña también se consideró la introducción del derecho a través de la vía judicial. La Corte Superior acabó rechazando dicha posibilidad.

cuando se produjo el segundo pronunciamiento de dicho tribunal. Por tanto, el efecto de irradiación europeo en materia de protección de datos conformó un régimen reforzado de protección en los anteriormente mencionados Estados latinoamericanos, sin que las garantías y las limitaciones introducidas por su desarrollo e interpretación jurisprudencial produjeran consecuencias similares⁴⁷.

En materia de transferencias internacionales de datos, el TJUE ocupa un papel similar, puesto que delimita el alcance de la protección por vía de este instrumento más allá de lo que preveía la norma, a través de sus sucesivos pronunciamientos en los asuntos *Schrems* y *Schrems II*, en cuanto a las relaciones entre la Unión y la normativa de protección de datos de EE. UU. que se habían establecido por vía decisonal de la Comisión Europea⁴⁸. En el momento en el que se producen esos pronunciamientos, solamente dos jurisdicciones latinoamericanas (la argentina en 2003⁴⁹ y la uruguay en 2012⁵⁰) habían sido reconocidas con un adecuado nivel de protección de datos personales por la Comisión Europea, a través de una decisión de adecuación⁵¹. El TJUE introduce un principio de equivalencia en estos pronunciamientos, frente al principio más atenuado de adecuación que regía en la época anterior a su sentencia⁵². Dada la divergencia del criterio interpretativo, solamente quince terceros países respecto de la Unión han sido reconocidos por la Comisión Europea a estos efectos —y ninguno más del ámbito latinoamericano—⁵³.

Ante esta situación, aquellos países que no habían obtenido una decisión de adecuación por parte de la Comisión Europea previa a estos pronunciamientos del TJUE, decidieron promulgar sus propias normas nacionales en materia de protección de datos, por los efectos irradiados por la Directiva de 1995, primero, y posteriormente por el RGPD⁵⁴. De hecho, gran parte de los países latinoamericanos regulan la transferencia de datos personales en sus propias normativas nacionales, principalmente a través de la influencia de la Red Iberoamericana de Protección de Datos, inspirándose en los principios de la regulación europea⁵⁵.

Aunque todas estas jurisdicciones toman el modelo de la Unión Europea, la adopción de sus propias normas nacionales en esta materia supuso también que podrían recuperar parte

47 Bradford, *The Brussels Effect*, 132-135.

48 Schwartz y Peifer, “Transatlantic Data Privacy Law”, 117.

49 European Commission, *Commission Decision of 30 June 2003 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Argentina*. 2003/490/EC, Brussels. <http://data.europa.eu/eli/dec/2003/490/oj> (accessed October 20, 2022).

50 European Commission, *Commission Implementing Decision of 21 August 2012 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the Eastern Republic of Uruguay with regard to automated processing of personal data*. 2012/484/EU, Brussels. http://data.europa.eu/eli/dec_impl/2012/484/oj (accessed October 20, 2022).

51 Bradford, *The Brussels Effect*, 149-152.

52 *Maximilian Schrems v Data Protection Commissioner*, Case C-362/14, para 97; *Data Protection Commissioner v. Facebook Ireland Limited and Maximilian Schrems*, Case C-311/18, párrs. 134-135.

53 “Adequacy decisions”, *European Commission*. Accessed October 19, 2022, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

54 Voss, “European Union Data Privacy Law Reform”, 222-223.

55 Red Iberoamericana de Protección de Datos, *Guía de implementación de cláusulas contractuales modelo para la transferencia internacional de datos personales*.

de su discreción al aplicar e interpretar estas mismas reglas⁵⁶. En ausencia de una normativa nacional, y sin una estructura institucional sólida que aplicara dicho régimen de protección, los criterios interpretativos relativos a la transferencia internacional de datos quedaban completamente a discreción de las autoridades de control europeas, así como de la Comisión Europea, por vía de decisión de adecuación.

EL IMPACTO DE LA LEY DE MERCADOS DIGITALES EN LATINOAMÉRICA

La base legal de la DMA es el artículo 114 del Tratado de Funcionamiento de la Unión Europea (TFUE). Es decir, el instrumento normativo trata de contrarrestar la fragmentación en el mercado interior producido por la segmentación de los modelos de negocio de las principales plataformas digitales en los distintos Estados miembros⁵⁷, los cuales han reaccionado a las prácticas anticompetitivas de estos operadores económicos de forma diferente: mientras que algunos han continuado aplicando el Derecho de la competencia con normalidad a través de sus propias normas nacionales, así como por vía de la aplicación directa de los artículos 101 y 102 TFUE, otros han optado por un papel más proactivo. Por ejemplo, algunos Estados miembros de la Unión como Alemania, Grecia, Italia y Austria han adaptado sus propias normas nacionales en materia de defensa de la competencia para capturar el fenómeno de las plataformas digitales de una forma más adecuada.

Este fenómeno ha generado segmentación en el mercado interior, puesto que dependiendo del Estado miembro en el que opere la plataforma digital debe sujetarse a unas normas de competencia distintas. En virtud de lo anterior, algunas conductas que podrían resultar prohibidas en sede alemana podrían ser aceptables en sede española, puesto que en el ámbito español no se ha promulgado ninguna norma para capturar de forma más precisa el fenómeno digital.

Dada esta situación, la DMA tiene un fin uniformizador de las reglas aplicables a las plataformas digitales en el mercado interior, predicables en el conjunto de los Estados miembros, y mantiene la complementariedad de los artículos 101 y 102 TFUE respecto de su aplicación⁵⁸. El problema que surge a raíz de esta tendencia unificadora es que estas plataformas digitales no operan en base a un modelo de negocio distinto dependiendo del territorio en el que se encuentren. De hecho, aplican el mismo modelo de negocio a nivel mundial, y posteriormente ajustan su conducta a las posibles limitaciones que cada régimen nacional les exija.

En la línea de la argumentación que se sigue en este artículo, se detectan tres principales ámbitos en los que la DMA puede producir situaciones de asimetría regulatoria en Latinoamérica, por lo que se refiere al funcionamiento de los mercados nacionales en relación con estas plataformas digitales.

56 Brian Nougères, "Chapter 7", 148-149. Por ejemplo, esto es lo que ha sucedido en California. Consumer Privacy Act §11.6 (2018) y el desarrollo en determinados estados de EE. UU, "US Federal Privacy Legislation Tracker", *IAPP*. Accessed May 15, 2023, <https://iapp.org/resources/article/us-federal-privacy-legislation-tracker/>.

57 Nicolaïdis y Howse, "This is my Eutopia...", 788.

58 European Parliament and Council. *Digital Markets Act*, Recital 7.

A. La designación de guardianes de acceso

La DMA se aplicará únicamente a determinados operadores digitales y no a todos ellos. El instrumento regulatorio diseña un proceso de designación que considera a determinados operadores económicos como guardianes de acceso, sin tener en cuenta las herramientas económicas relativas a la definición del mercado relevante, propias de la aplicación pública del Derecho de la competencia. La DMA introduce esta nomenclatura para indicar qué sujetos deberán ajustar su comportamiento competitivo y sus modelos de negocio a su articulado. La designación se realiza en base a criterios cualitativos y cuantitativos⁵⁹. Es decir, la Comisión Europea tendrá en cuenta dimensiones tales como el número de usuarios integrados en la plataforma o su capitalización bursátil, sin perjuicio de que deben prestar sus servicios en al menos tres Estados miembros para verse sujetos por la regulación. Por tanto, la DMA se aplicará en función de la vinculación de estas plataformas digitales con el mercado interior europeo. Sin embargo, la repercusión de sus disposiciones se proyectará al resto de jurisdicciones mundiales.

Por el momento, la Comisión ha comunicado que hasta siete plataformas digitales le han notificado su potencial designación como guardianes de acceso, incluyendo las norteamericanas Google, Apple, Amazon y Microsoft, la china ByteDance y la surcoreana Samsung.

Desde la perspectiva de la designación, este hecho puede generar unos elevados costes de distribución sobre determinados operadores económicos que pueden caer bajo la denominación de guardián de acceso de la DMA, pero que no ocupen esta situación predominante extramuros de la Unión.

A pesar de que la DMA está orientada a corregir las situaciones de falta de disputabilidad e inequidad en el seno de las plataformas digitales, los efectos distributivos del instrumento regulatorio resultan desproporcionados respecto de sus efectos en el resto de las jurisdicciones del mundo. Los designados “guardianes de acceso”, que estén entrando a los mercados latinoamericanos, tendrán que afrontar unos costes añadidos por su presencia y su posición destacada en el mercado interior europeo, a pesar de que este hecho no tiene ninguna conexión con su situación competitiva real en el mercado latinoamericano⁶⁰.

B. La imposición del estándar global más elevado de protección

Una vez se ha completado la designación del guardián de acceso, este se ve limitado automáticamente por una serie de obligaciones y prohibiciones a las que se debe ajustar en un plazo de seis meses a partir de la designación⁶¹.

Por una parte, el guardián de acceso debe respetar las prohibiciones establecidas en el artículo 5 de la DMA respecto de determinadas conductas que se consideran nocivas para la disputabilidad y equidad de los mercados digitales. Por ejemplo, el artículo 5(3) prohíbe las conductas de autofavorecimiento dirigidas contra los competidores del guardián de acceso,

59 European Parliament and Council. *Digital Markets Act*, Article 3(2).

60 “Distributional Effects and Benefit-Cost Analysis”.

61 European Parliament and Council. *Digital Markets Act*, Article 3(10).

sin perjuicio de que en materia de competencia sus contornos aún no hayan sido perfectamente delimitados.

Por otra parte, los artículos 6 y 7 de la DMA establecen toda una serie de obligaciones que el operador digital debe cumplir. El artículo 6, por ejemplo, prevé obligaciones especialmente relacionadas con el uso intensivo de datos en su modelo de negocio, y el artículo 6(9), partiendo de su definición en el artículo 20 del GDPR, amplía el espectro del derecho a la portabilidad de los datos⁶² de los usuarios finales de las plataformas digitales, estableciendo que su ejercicio efectivo se debe producir en el marco de un acceso continuo y en tiempo real. En el ámbito latinoamericano este cambio normativo aumentará la protección de los usuarios finales, al poder beneficiarse de un derecho a la portabilidad de sus datos no solamente personales, sino mucho más allá de los contornos que han delimitado sus propias normativas nacionales en materia de protección de estos.

Las obligaciones en materia de interoperabilidad⁶³ previstas en el artículo 7 de la DMA aplican particularmente a aquellos guardianes de acceso que prestan servicios de comunicaciones interpersonales independientes de la numeración (por ejemplo, WhatsApp). Y de acuerdo con lo previsto en el artículo 7(2)(a)(i), los guardianes de acceso deberán asegurar que los mensajes de texto entre dos usuarios finales individuales sean interoperables. En materia regulatoria esta es una de las reformas que tendrán un mayor impacto en la vida diaria de los usuarios de las plataformas digitales. En razón de lo anterior, un usuario que utilice WhatsApp deberá poder mensajearse con un usuario de otro proveedor, por ejemplo, de Signal o Telegram, sin necesidad de instalar esta segunda aplicación en su dispositivo. Considerando la popularidad de estos servicios de mensajería en Latinoamérica, la DMA proyectará sus efectos directamente en la vida diaria de los usuarios finales latinoamericanos⁶⁴.

A partir de su futura entrada en vigor y su aplicación, la DMA fija el estándar de protección más elevado respecto de los guardianes de acceso. Es difícil imaginar que estas plataformas digitales apliquen un modelo de negocio distinto a nivel europeo respecto de aquel que emplean en el resto del mundo, dada la gran inversión requerida para acatar la nueva norma europea. A medida que la DMA sea exigible a nivel europeo comenzará a permear sus efectos en las distintas jurisdicciones en las que estas plataformas digitales ya tienen un elevado grado de implantación.

El principal problema de estos efectos reflejos de la DMA en Latinoamérica es que, a pesar de que se proyecten sus obligaciones en el territorio, la autoridad encargada de supervisar su cumplimiento y de sancionar sus potenciales incumplimientos seguirá siendo la Comisión Europea⁶⁵, en ausencia de una norma nacional que replique sus disposiciones en el ámbito

62 De acuerdo con el Considerando 59 de la DMA, el derecho a la portabilidad de este instrumento normativo se refiere al derecho de los usuarios finales al acceso efectivo e inmediato a los datos que hayan proporcionado o generado a través de sus actividades en los servicios del guardián de acceso. El artículo 20 del RGPD regula el mismo derecho, pero sin las características de que se produzca un acceso definido de forma “inmediata y efectiva”.

63 La interoperabilidad se refiere a la capacidad de comunicación entre dos sistemas técnicos distintos. Si no existe interoperabilidad, ambos sistemas no pueden comunicarse y, por lo tanto, los usuarios finales no pueden utilizar varios servicios provistos por operadores distintos de la misma naturaleza, tal y como señala el Considerando 64 de la DMA.

64 “¿Qué tan popular es WhatsApp en Latinoamérica?”.

65 European Parliament and Council. *Digital Markets Act*, Chapter V.

interno. De esta forma, existe el riesgo evidente de que las obligaciones de la DMA se proyecten de forma defectuosa en las jurisdicciones distintas a la propia Unión, puesto que el resto de territorios escapan del ámbito de control de la Comisión Europea.

Desde la perspectiva latinoamericana, las propias autoridades nacionales de competencia, regulatorias y de protección del consumidor tampoco estarán legitimadas para aplicar y monitorizar extraterritorial y directamente las disposiciones de la DMA. Por tanto, las ‘bondades’ que la DMA pueda proyectar sobre los usuarios latinoamericanos pueden verse rápidamente enturbiadas por una falta de supervisión directa de sus disposiciones.

C. Los procesos sancionadores por incumplimiento de la DMA frente a la aplicación pública del Derecho de la competencia

La DMA, en cuanto norma regulatoria dirigida a unos determinados operadores económicos, se aplicará por parte de la Comisión Europea de forma simultánea a su propio conocimiento de expedientes sancionadores en materia de competencia. Como el instrumento regulatorio se inspira en la propia experiencia de la Comisión Europea, en los procedimientos sancionadores sobre los que ya ha decidido en materia de competencia podría darse la posibilidad de que una misma plataforma digital pueda verse sujeta a dos obligaciones similares, por ejemplo, la prohibición de autofavorecimiento y, simultáneamente, límites y condiciones distintas en función del ámbito del que provengan⁶⁶.

En relación con los efectos extraterritoriales de la DMA, el problema de la duplicación y la interacción de los procedimientos por incumplimiento de la norma regulatoria y de los expedientes sancionadores en materia de competencia son aún mayores que en el caso de la Comisión Europea. En su Considerando 86, la DMA contempla que las multas que se puedan imponer como consecuencia de su incumplimiento deben respetar los principios de proporcionalidad y *non bis in idem* para evitar el solapamiento con aquellos procedimientos sancionadores en materia de competencia en manos de la Comisión o de las autoridades nacionales competentes⁶⁷.

Sin embargo, nada se dice respecto de la posible interacción de la DMA con el resto de los procedimientos que ahora mismo se encuentran en marcha por causa de fallos de mercados similares a los que la propia DMA quiere atender en las distintas jurisdicciones del mundo. Aunque los procedimientos en los que se ha sancionado la conducta unilateral de las plataformas digitales en el ámbito latinoamericano son escasas⁶⁸, este fenómeno no es ni mucho menos residual. En este sentido, el 30 de septiembre de 2022, la Comisión Federal de Competencia Económica (COFECE) incoó un procedimiento sancionador para dilucidar el carácter anticompetitivo de los operadores económicos en el trasfondo de las aplicaciones móviles⁶⁹, siguiendo la tendencia general mejicana de capturar el fenómeno digital desde una perspectiva nacional⁷⁰. Poco después, el 19 de octubre de 2022, la Fiscalía Nacional Económica

66 “An Inverse Analysis of the DMA”.

67 Ribera Martínez, “An Inverse Analysis of the Digital Markets Act”.

68 “Plataformas digitales y Derecho de la competencia”.

69 “Cofece investiga posibles prácticas monopólicas”.

70 OCDE, *Digital Platforms and Competition in Mexico 2018*.

chilena resolvió que existe mérito para investigar las conductas anticompetitivas ejecutadas en la distribución de aplicaciones mediante la App Store y Google Play⁷¹. Como podemos suponer, los resultados que arrojen estas investigaciones pueden ser idénticos a aquellos que ya ha señalado la DMA, mientras que sus soluciones pueden distar de las obligaciones concretamente establecidas en virtud del instrumento regulatorio europeo.

Ante esta situación, las autoridades de competencia tendrán tres opciones. En primer lugar, aplicar su régimen nacional en lo referente a la imposición de obligaciones, en caso de que se detecte una conducta anticompetitiva, independientemente de las obligaciones previstas en la DMA. En segundo lugar, aplicar su régimen nacional con una clara inspiración en las obligaciones previstas en la DMA, para tratar de acomodar su respuesta a los cambios en los modelos de negocio que presenta la normativa regulatoria. Por último, aplicar su régimen nacional yendo incluso más allá del régimen de protección previsto por la DMA. En coherencia con el principio de proporcionalidad, las autoridades latinoamericanas podrían acomodar su propia actuación a lo que ya está previsto en la DMA, tratando de conseguir una protección equivalente para sus usuarios nacionales en sus propias jurisdicciones, e incluso una protección superior a la que el instrumento regulatorio impone. Sin embargo, este ejercicio viene precedido de un paso anterior: el reconocimiento de la DMA como un instrumento regulatorio con efectos extraterritoriales plenos en Latinoamérica, que debe considerarse inserto en el amplio acervo de los instrumentos que las autoridades nacionales de competencia tienen a su disposición.

CONCLUSIONES

El impacto de la normativa europea en el resto de las jurisdicciones mundiales, en cuanto a su nivel de protección, es indudable. La *vis atractiva* de la capacidad de consumo del conjunto de los consumidores europeos sigue siendo un elemento clave para que el tejido empresarial traslade los estándares europeos al desarrollo de sus actividades mundiales. Además, en muchas ocasiones, por la naturaleza de la propia materia de la que se trate, a dichos operadores económicos les resulta más eficiente aplicar el mismo nivel (elevado) de protección en todas las jurisdicciones en las que operan, que segmentar el desarrollo de sus actividades en función de la legislación nacional aplicable.

Este fenómeno es el que, precisamente, ha impregnado la difusión de la normativa europea de protección de datos personales al resto de las jurisdicciones del mundo en lo referente tanto al contenido de la Directiva de 1995 como a los estándares que introdujo el RGPD. Dos de los grandes ámbitos en los que se ha producido un mayor progreso por vía jurisprudencial han sido: i) el derecho al olvido y ii) la virtualidad de las transferencias internacionales de datos. A pesar de que estos avances son sustantivos en cuanto a su impacto, tanto la aplicación como la interpretación de sus normas siguen quedando en manos de las autoridades europeas, en ausencia de legislación nacional aplicable, con el consiguiente impacto desfavorable en su soberanía.

71 Fiscalía Nacional Económica, *Resolución N.º 26/19-10-2022*, Accessed October 28, 2022 (in file with author).

A partir de estos riesgos, en este artículo se detectan tres grandes ámbitos de conflicto que se generarán en torno a la futura aplicación de la DMA en territorio europeo y, por extensión, a nivel mundial.

En primer lugar, la designación de los principales operadores digitales generará desigualdades en Latinoamérica, puesto que algunos de los guardianes de acceso serán designados por su predominancia europea, no tendrán esa misma relevancia en estos países y, de esta forma, se generará una clara desventaja competitiva en su entrada a los mercados latinoamericanos. El mismo problema operará a la inversa, es decir, aquellos operadores económicos exclusivamente latinoamericanos que escapen del ámbito de protección de la DMA, no estarán en un plano de igualdad con los operadores económicos limitados por el instrumento regulatorio.

En segundo lugar, las prohibiciones y las obligaciones de la DMA se impondrán en los modelos de negocio de los guardianes de acceso a nivel mundial, sin que las autoridades latinoamericanas puedan actuar frente a sus criterios interpretativos y a la supervisión de su cumplimiento. Aunque la aplicación de las disposiciones de la DMA conferirá a los usuarios latinoamericanos un mayor nivel de protección, las autoridades nacionales no podrán detectar ni sancionar las desviaciones de su conducta que se produzcan en este ámbito regulatorio.

En último lugar, la aplicación pública en materia de competencia se verá comprometida por los efectos de la DMA, puesto que se podrán dar solapamientos entre los procedimientos sancionadores existentes en el ámbito latinoamericano contra estas mismas plataformas digitales, y aquellos procedimientos regulatorios que se implementarán como consecuencia del instrumento regulatorio europeo.

BIBLIOGRAFÍA

1. Bach, David y Abraham L. Newman. "The european regulatory state and global public policy: micro-institutions, macro-influence". *Journal of European Public Policy* núm. 14 (1 de septiembre de 2007): 827–46. <https://doi.org/10.1080/13501760701497659>
2. Bergkamp, Lucas. "EU data protection policy: the privacy fallacy: adverse effects of Europe's data protection policy in an information-driven economy". *Computer Law & Security* 18, núm. 1 (31 de enero de 2002): 31–47, [https://doi.org/10.1016/S0267-3649\(02\)00106-1](https://doi.org/10.1016/S0267-3649(02)00106-1)
3. Bradford, Anu. *The Brussels effect: How the European Union rules the world*. New York: Oxford University Press, 2020. <https://www.oxfordscholarship.com/view/10.1093/oso/9780190088583.001.0001/oso-9780190088583>
4. Bradford, Anu. "The Brussels Effect" *Northwestern University Law Review* 107, no. 1 (2012): 1-64.
5. Brian Nougrères, Ana. "Chapter 7: Data protection and enforcement in Latin America and in Uruguay". In *Enforcing privacy: Regulatory, legal and technological approached*, edited by David Wright and Paul De Hert, 145-182. Switzerland: Springer, 2017.
6. Carter, Edward L. "Argentina's right to be forgotten". *Emory International Law Review* 27, núm. 1 (2013): 23–39. <https://scholarlycommons.law.emory.edu/cgi/viewcontent.cgi?article=1097&context=eilr>
7. Center for Health Decision Science. "Distributional Effects and Benefit-Cost Analysis". Accessed October 20, 2022. <https://chds.hsph.harvard.edu/distributional-effects-and-benefit-cost-analysis/>

8. Cofece. "Cofece investiga posibles prácticas monopólicas relativas en el mercado de desarrollo, distribución y procesamiento de pagos de aplicaciones móviles y contenido digital, así como servicios relacionados". Accessed October 21, 2022. <https://www.cofece.mx/cofece-investiga-posibles-practicas-monopolicas-relativas-en-mercado-de-pagos-de-aplicaciones-moviles-y-contenido-digital/>.
9. Damro, Chad. "Market power Europe". *Journal of European Public Policy* 19, núm. 5 (2012): 682-99. <https://doi.org/10.1080/13501763.2011.646779>
10. Frosio, Giancarlo F. "The right to be forgotten: much ado about nothing". *Colorado Technology Law Journal* 15, núm. 2 (2017): 307-36. <https://ssrn.com/abstract=2908993>
11. Google. "European Union Consumer Spending". *Trading Economics*. Accessed October 11, 2022. <https://tradingeconomics.com/european-union/consumer-spending>
12. Google. "United States Indicators". *Trading Economics*. Accessed October 11, 2022. <https://tradingeconomics.com/united-states/indicators>
13. Google. "China Indicators". *Trading Economics*. Accessed October 11, 2022. <https://tradingeconomics.com/china/indicators>.
14. Ibáñez Colomo, Pablo. "The Draft Digital Markets Act: A Legal and Institutional Analysis". *Journal of European Competition Law & Practice* 12, núm. 7 (1 de septiembre de 2021): 561-75. <https://doi.org/10.1093/jeclap/lpab065>.
15. Kogan, Lawrence A. "Exporting Europe's Protectionism". *The National Interest* No. 77 (2004): 91-99, <https://www.jstor.org/stable/42895696>
16. La Libre Competencia. "Plataformas digitales y Derecho de la competencia en América Latina y el Caribe". Accessed October 21, 2022. <https://lalibrecompetencia.com/2020/11/15/plataformas-digitales-y-derecho-de-la-competencia-en-america-latina-y-el-caribe/>.
17. Lam, Christina. "Unsafe Harbor: The European Union's Demand for Heightened Data Privacy Standards in *Schrems v. Irish Data Protection*". *Boston College International & Comparative Law Review* No. 40 (2017): 1-13. <https://core.ac.uk/download/pdf/80398884.pdf>
18. Mariniello, Mario y Martins, Catarina. "Which platforms will be caught by the Digital Markets Act? The 'gatekeeper' dilemma". *Bruegel*. Accessed October 20, 2022. <https://www.bruegel.org/blog-post/which-platforms-will-be-caught-digital-markets-act-gatekeeper-dilemma>.
19. Martínez Herrera, Manuel. "From *Habeas Data* Action to *Omnibus* Data Protection: The Latin American Privacy (R)Evolution". *White & Case*. Accessed October 22, 2022. https://www.whitecase.com/sites/default/files/files/download/publications/article_from_habeas_data_action_to_omnibus_data_protection.pdf2_.pdf.
20. Nicolaïdis, Kalypso and Robert Howse. "'This is my Eutopia...': Narrative as Power". *Journal of Common Market Studies* No. 40 (2002): 767-792, <https://ssrn.com/abstract=342785>
21. Oracle. "Oracle expande su presencia global de regiones de nube para apoyar la aceleración digital de las organizaciones". Accessed October 20, 2022. <https://www.oracle.com/lat/news/announcement/oracle-expands-global-cloud-footprint-to-meet-continued-triple-digit-growth-2021-10-11/>.
22. Organización para la Cooperación y el Desarrollo Económicos (OCDE). Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Council of Europe. Convention No. 108 on data protection (ETS No. 108, 28.01.1981).

23. Organización para la Cooperación y el Desarrollo Económicos. *Digital Platforms and Competition in Mexico 2018*. Accessed October 21, 2022. <https://www.oecd.org/daf/competition/eng-digital-platforms-and-competition-in-mexico.pdf> ().
24. Petit, Nicolas. "The Proposed Digital Markets Act (DMA): A Legal and Policy Review". *Journal of Competition law & Practice* No. 12 (2021): 529-541. <https://doi.org/10.1093/jeclap/lpab062>
25. Puccinelli, Oscar Raúl. "Evolución histórica y análisis de las diversas especies, subespecies, tipos y subtipos de habeas data en América Latina: Un intento clasificador con fines didácticos". *Vuniversitas* No. 107 (2004): 472-4501. <https://content.lpderecho.pe/wp-content/uploads/2021/07/Evoluci%C3%B3n-hist%C3%B3rica-de-H%C3%A1beas-Data-en-Am%C3%A9rica-Latina.-Oscar-Ra%C3%BAl-Puccinelli.pdf>
26. Kluwer Competition Law Blog. "An Inverse Analysis of the DMA: Amazon's Proposed Commitments to the European Commission". Accessed October 21, 2022. <http://competitionlawblog.kluwercompetitionlaw.com/2022/07/27/an-inverse-analysis-of-the-dma-amazons-proposed-commitments-to-the-european-commission/>.
27. Red Iberoamericana de Protección de Datos. *Guía de implementación de cláusulas contractuales modelo para la transferencia internacional de datos personales*. <https://www.redipd.org/sites/default/files/2021-11/red-iberoamericana-guia-implementacion-scc-2021.pdf>.
28. Ribera Martínez, Alba, "An Inverse Analysis of the Digital Markets Act: Applying the Ne Bis in Idem Principle to Enforcement". *European Competition Journal* No. 19 (2023): 86-115. <https://www.tandfonline.com/doi/abs/10.1080/17441056.2022.2156729?journalCode=recj20>
29. Schwartz, Paul M. y Karl-Nikolaus Peifer. "Transatlantic Data Privacy Law". *The Georgetown Law Journal* No. 106 (2017): 117-178. https://www.law.georgetown.edu/georgetown-law-journal/wp-content/uploads/sites/26/2019/10/Transatlantic-Data-Privacy-Law_Schwartz-and-Peifer.pdf.
30. Shaffer, Gregory. "Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards". *The Yale Journal of International Law* No. 25 (2000): 1-80. <https://ssrn.com/abstract=531682>.
31. Spar, Debora L. y David B. Yoffie. "A Race to the Bottom or Governance from the Top?" In *Coping with Globalization*, editado por Aseem Prakash y Jeffrey A. Hart, 31-51. London: Routledge, 2000.
32. Statista. "¿Qué tan popular es WhatsApp en Latinoamérica?". Accessed October 21, 2022. <https://es.statista.com/grafico/17500/uso-de-whatsapp-en-america-latina/>
33. Voss, W. Gregory. "European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting". *The Business Lawyer* No. 72 (2017): 221-233, <https://ssrn.com/abstract=2894571>
34. Zalando. "Zalando group financials as of Q2/22". Accessed October 20, 2022. https://corporate.zalando.com/sites/default/files/media-download/Zalando%20SE%20Q2%202022%20Financials%20PDF_1.pdf
35. Zamudio Salinas, María de Lourdes. "El marco normativo latinoamericano y la Ley de protección de datos personal del Perú". *Revista Internacional de Protección de Datos Personales* No. 1 (2012): 2-21. https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/ok3_Ma.-de-Lourdes-Zamudio_FINAL.pdf