LA APLICACIÓN EXTRATERRITORIAL DEL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

La aplicación extraterritorial del Reglamento General de Protección de Datos

El Reglamento General de Protección de Datos introdujo reglas de aplicación extraterritorial por las que organizaciones ubicadas fuera de la Unión Europea pueden quedar sujetas a su aplicación, incluido su régimen sancionador. En este artículo se analiza el alcance de estas reglas, así como la opinión de las autoridades europeas sobre el alcance de la aplicación territorial.

Analysis of the extraterritorial scope of GDPR

General Data Protection Regulation introduced rules regarding the extraterritorial applicability of its rules, according to which organizations located outside the European Union may be subject to it, including its sanctioning regime. This articles provides for an analysis of the scope of the extraterritorial applicability, as well as of the opinion of the competent EU authorities on this territorial scope.

Palabras clave

Protección de datos, privacidad, RGPD, extraterritorialidad, cookies

Key words

Data protection, privacy, GDPR, extraterritorial scope, cookies

Fecha de recepción: 22-07-2019 *Fecha de aceptación: 01-09-2019*

Una de las principales —y más publicitadas y debatidas— novedades que introdujo el Reglamento General de Protección de Datos (Reglamento UE 2016/679, o "RGPD") fue la ampliación del ámbito de aplicación territorial de las normas europeas de protección de datos respecto al ámbito que se establecía en la normativa inmediatamente precedente (i. e., la Directiva 95/46/CE y las correspondientes normas de transposición nacionales). La principal novedad en este sentido se produjo, en particular, con la introducción de reglas específicas de extraterritorialidad en la aplicación del RGPD. Estas reglas, que se encuentran en el apartado 2 del artículo 3 del RGPD, establecen una serie de supuestos en los que responsables o encargados del tratamiento de datos personales que estén ubicados fuera de la Unión Europea (UE) pueden quedar sujetos a las reglas establecidas en el RGPD, a la monitorización de los tratamientos por parte de las autoridades de los Estados miembros de la UE y a su régimen sancionador.

El artículo 3 del RGPD señala lo siguiente respecto al ámbito de aplicación territorial de la norma de protección de datos:

"*Artículo 3.* Ámbito *territorial*

1.El presente Reglamento 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.

2.El presente Reglamento se aplica al tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con:

a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o

b) el control de su comportamiento, en la medida en que este tenga lugar en la Unión.

3.El presente 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".

La introducción de estas reglas de extraterritorialidad en el RGPD no hizo sino confirmar una tendencia que ya se estaba consolidando en la UE y que implicaba una creciente exigibilidad del cumplimiento de las normas de protección de datos europeas a aquellas entidades que, con independencia de su ubicación y nacionalidad, llevaban a cabo actividades empresariales en la UE con acceso a, y tratamiento de, datos personales de ciudadanos de la UE. Esta tendencia interpretativa traía causa en la digitalización cada vez más evidente de muchos sectores y negocios, lo que facilitaba enormemente el acceso al mercado de usuarios finales europeos a entidades extracomunitarias sin que tuvieran necesidad de ubicar recursos físicos o filiales en la UE. En este sentido, con anterioridad al 25 de mayo de 2018 —fecha en la que se inició la apli-

López-Lapuente, Leticia: "La aplicación extraterritorial del Reglamento General de Protección de Datos", *Actualidad Jurídica Uría Menéndez*, 52, 2019, pp. 136-140 (ISSN: 1578-956X).

cación del RGPD—, y pese a que la Directiva 95/46/CE no contenía reglas de extraterritorialidad, diversas autoridades de protección de datos en el territorio de la UE, así como el Tribunal de Justicia de la UE ("TJUE") a partir de la Sentencia C-131/12 en el caso Google vs. Costeja, habían ampliado *de facto* el ámbito de aplicación territorial de las normas europeas a entidades ubicadas fuera de la UE al dictar diversas resoluciones y sentencias en aplicación de las normas de protección de datos frente a entidades no europeas.

El ámbito de aplicación territorial natural y primario del RGPD es el que establece su artículo 3.1, que dicta que el RGPD será de aplicación a aquellos tratamientos de datos personales que se realicen "*en el contexto de las actividades de un establecimiento*" del responsable o del encargado en la UE. Merece la pena destacar que no se exige, por tanto, la existencia de una sociedad (u otra entidad con una forma jurídica concreta) de nacionalidad europea, sino que para que el RGPD sea aplicable basta con que exista un "establecimiento" en la UE. La interpretación del concepto de "establecimiento" por parte de las autoridades europeas, incluyendo la Agencia Española de Protección de Datos ("AEPD"), ha sido extensiva y comprenderá, por ejemplo, sucursales o establecimientos a efectos fiscales, puesto que el considerando 22 del RGPD aclara que un establecimiento implica simplemente el ejercicio de manera efectiva y real de una actividad "*a través de modalidades estables*" y que la forma jurídica que revistan tales modalidades no es el factor determinante al respecto.

Esta interpretación extensiva del concepto de "establecimiento" ha sido confirmada tanto por el TJUE (p. ej., en el caso C- 230/14, Weltimmo vs. NAIH) como por el Comité Europeo de Protección de Datos (*European Data Protection Board* o "EDPB"), este último en la Guía 3/2018 sobre la aplicación territorial del RGPD que hizo pública en noviembre de 2018 (la "Guía"). En ella, el EDPB confirma que, sin perjuicio del requisito de una cierta estabilidad que es exigible a los establecimientos para ser considerados como tales bajo el RGPD, basta con que ejerzan una actividad real y efectiva "*mínima*" para que pueda activarse la aplicación del RGPD, sobre todo en los negocios *online*. En la Guía se señala a este respecto que, por ejemplo, la presencia de un único empleado o agente ubicado en la UE podría resultar suficiente ("*As a result, in some circumstances, the presence of one single employee or agent of the non-EU entity may be sufficient to constitute a stable arrangement if that employee or agent acts with a sufficient degree of stability*").

Deberá existir un establecimiento, aunque sea con una actividad limitada. Pese a esta interpretación extensiva, el EDPB aclara con buen criterio en la Guía que el hecho de que un responsable no europeo contrate y se sirva de los servicios de un encargado (i. e., prestador de servicios) ubicado en la UE no da como resultado la aplicación del RGPD al responsable. Debe cumplirse con el requisito de la existencia de un establecimiento para que se aplique el artículo 3.1 del RGPD, y no basta entonces con que se contrate a un prestador de servicios ubicado en la UE.

Capítulo aparte exigiría el análisis de la literalidad del artículo 3.1 del RGPD, cuando señala que para que el RGPD sea aplicable basta con que los tratamientos se realicen "*en el contexto*" de las actividades del establecimiento europeo. Baste apuntar sumariamente que esta redacción, que está en línea con la interpretación del TJUE en sentencias como la anteriormente citada en el caso C-131/12 (Google vs. Costeja), amplía la aplicabilidad del RGPD no solamente a tratamientos de datos realizados directamente por el establecimiento europeo, sino también a otros realizados en el contexto de su actividad.

Por último, en el apartado 1 del artículo 3 también se aclara que el RGPD será exigible a todo tratamiento realizado por el establecimiento europeo, con independencia de que el tratamiento de los datos —su recogida, almacenamiento, etc.— tenga lugar en la UE o no. Por ello, no es posible excluir de la aplicación del RGPD aquellos tratamientos que responsables o encargados europeos realicen fuera de la UE, bien porque la actividad empresarial o profesional se ejecute y tenga lugar fuera de la UE, o bien porque los datos se ubiquen y almacenen fuera de la UE.

Analizado el ámbito de aplicación territorial natural del RGPD (i. e., los tratamientos realizados por establecimientos europeos), conviene analizar las reglas propiamente extraterritoriales, que buscan de forma expresa la aplicación de la norma europea a responsables o encargados no nacionales de Estados miembros. Nos encontramos entonces ante la posible aplicación del RGPD a organizaciones no europeas, incluso en el caso de que estas organizaciones no cuenten con establecimiento alguno en la UE. Este análisis es relevante, puesto que la aplicación del RGPD en una organización es compleja y exige numerosas actuaciones en materia de transparencia a los interesados respecto al tratamiento de sus datos personales, requisitos de seguridad y

organización interna, etc. Por ello, si se determina que una entidad no europea debe cumplir con el RGPD con arreglo a estas reglas extraterritoriales, la aplicación del RGPD exigirá a dicha organización una adaptación significativa de procedimientos y sistemas que conllevará la dedicación, esfuerzos y recursos organizativos y económicos.

Los casos en los que el apartado 2 del artículo 3 del RGPD determina que será de aplicación el RGPD de manera extraterritorial a tratamientos de datos personales de interesados que residan en la UE por parte de cualquier responsable o encargado no establecido en la UE son los siguientes:

a) cuando el tratamiento de los datos esté relacionado con la oferta de bienes o servicios a interesados en la UE, independientemente de si a estos se les requiere su pago, o

b) cuando el tratamiento de los datos esté relacionado con el control del comportamiento de los interesados, en la medida en que este tenga lugar en la UE.

Una regla extraterritorial adicional es la que se prevé en el apartado 3 del artículo 3 del RGPD, por la que se establece que el Reglamento se aplicará al tratamiento de datos personales por parte de responsables no establecidos en la UE si se ubican en un lugar en que el derecho de los Estados miembros sea de aplicación en virtud del derecho internacional público.

Dejando al margen del análisis este último supuesto (i. e., aquellos casos de aplicabilidad por razón de derecho internacional público), las organizaciones y el tejido empresarial no europeo se plantean recurrentemente cuál es el alcance del apartado 2 del artículo 3 del RGPD o, lo que es lo mismo, en qué casos las autoridades y tribunales entenderán que una organización no europea está realizando oferta de bienes y servicios o monitorizando el comportamiento de interesados (i. e., personas físicas cuyos datos son objeto de tratamiento) en la UE. Los supuestos se definen en el apartado 2 del artículo 3 del RGPD de una forma general y algo ambigua, dejando margen a diversas interpretaciones que generan inseguridad jurídica respecto al ámbito de aplicación de la norma.

Un primer criterio interpretativo se encuentra en el propio RGPD, puesto que, entre sus considerandos, tanto el 23 como el 24 pretenden aportar algo de luz a los criterios generales del artículo 3.2 del RGPD. El considerando 23, además de destacar que la extraterritorialidad del RGPD tiene como finalidad garantizar que las personas físicas no se vean privadas de la protección a la que tienen derecho en virtud de esta norma, interpreta algo más específicamente el concepto de oferta de bienes o servicios a los interesados. En particular, señala que, para determinar si un responsable o encargado ofrece bienes o servicios a interesados que residen en la UE, debe estarse a un criterio de materialidad, es decir, si "*es evidente*" que el responsable o el encargado "*proyecta ofrecer servicios a interesados en uno o varios de los Estados miembros de la Unión*". Por ello, se excluirían del ámbito de aplicación situaciones en las que, excepcionalmente y sin intención del responsable o encargado, un bien o un servicio terminan siendo ofertados en la UE. En este sentido, la intención de la organización no europea de ofrecer esos bienes o servicios a interesados de la UE deviene un criterio relevante a los efectos de determinar la aplicabilidad del RGPD.

En este sentido, el considerando 23 aporta otro criterio interpretativo relevante cuando señala que la mera accesibilidad del sitio web del responsable o encargado (o de un intermediario), de una dirección de correo electrónico u otros datos de contacto, o el uso de una lengua generalmente utilizada en el tercer país donde resida el responsable, no bastarían para determinar esa intención de la organización no europea de ofrecer los bienes y servicios en la UE. Por tanto, por ejemplo, el mero hecho de que una web esté disponible en castellano por tratarse de una organización, pongamos por caso, mexicana, no es relevante para determinar que se está ofreciendo a ciudadanos en España ni activa automáticamente la aplicabilidad del RGPD. Sin embargo, el propio considerando 23 apunta que hay factores, considerados solos o conjuntamente, como el uso de una lengua o una moneda utilizada generalmente en uno o varios Estados miembros con la posibilidad de encargar bienes y servicios en esa otra lengua, o la mención de clientes o usuarios que residen en la UE, que pueden revelar que el responsable del tratamiento sí proyecta y tiene la intención de ofrecer bienes o servicios a interesados en la UE. La Guía del EDPB proporciona criterios interpretativos adicionales y ejemplos concretos respecto a qué se entiende por oferta de bienes y servicios en el sentido del artículo 3.2.a) del RGPD.

Una pregunta recurrente al analizar estas cuestiones es a qué se refiere el artículo 3 del RGPD al referirse a "*interesados en la Unión*" como sujetos respecto de los que el tratamiento de sus datos personales activaría la aplicabilidad del RGPD. La duda más recu-

rrente sobre este aspecto es si el RGPD se refiere a ciudadanos nacionales de Estados miembros de la UE, si basta con que tengan estatus jurídico de residentes en el territorio de la UE con independencia de su nacionalidad o si basta con que los interesados se encuentren localizados "en" la UE con independencia de su estatus jurídico. En este sentido, el RGPD parece referirse a ciudadanos localizados en la UE, puesto que no sujeta la aplicación de la norma a un requisito de nacionalidad o residencia legal. Esta interpretación amplia ha sido confirmada en la Guía. La precisión es relevante, por ejemplo, en la medida que existen ciudadanos nacionales de un Estado miembro que residen fuera de la UE y, en muchos casos, organizaciones no europeas se plantean si el tratamiento de los datos de esos nacionales europeos residentes en el país de origen del propio responsable (p. ej., porque se abran una cuenta en una entidad de crédito en el país no UE) activaría la aplicación del RGPD. En estos supuestos, la Guía aclara expresamente que no sería de aplicación el RGPD.

Más complejo aún se hace determinar el alcance concreto del supuesto de extraterritorialidad previsto en el artículo 3.2.b) del RGPD ("*el control de su comportamiento, en la medida en que este tenga lugar en la Unión*"). El concepto de "control de comportamiento" es complejo, indeterminado y sujeto a muy diversas interpretaciones. El considerando 24 del RGPD elabora algo más este concepto y señala que este supuesto debe entenderse aplicable "*cuando esté relacionado con la observación del comportamiento de dichos interesados*" en la medida en que este comportamiento tenga lugar en la UE. Por tanto, como el propio EDPB aclara en la Guía, el requisito para este supuesto es doble: debe referirse a interesados ubicados en la UE y el comportamiento monitorizado debe tener lugar y desarrollarse por dicho interesado también en el territorio de la UE.

Para determinar si se puede considerar que un tratamiento "*controla*" el comportamiento de los interesados, el considerando 24 señala que debe tenerse en consideración si las personas físicas son objeto de un seguimiento en Internet, "*inclusive el potencial uso posterior de técnicas de tratamiento de datos personales que consistan en la elaboración de un perfil de una persona física con el fin, en particular, de adoptar decisiones sobre él o de analizar o predecir sus preferencias personales, comportamientos y actitudes*". Sin embargo, y a pesar de la expresa referencia del considerando 24 al seguimiento de comportamientos a través de Internet, el EDPB ha manifestado en la Guía que no debe darse una interpretación estricta al artículo y deberían considerarse también monitorizaciones realizadas por redes y tecnologías distintas a Internet.

Existe el riesgo de una interpretación expansiva del supuesto del artículo 3.2.b) del RGPD, consistente en que cualquier recogida de datos personales por medios *online* y su posterior análisis, a través, por ejemplo, de cualquier sitio web o *app*, implique la aplicación del RGPD a entidades no europeas. En este sentido, el EDPB ha querido aclarar en la Guía su interpretación, y señala que no considera que cualquier recogida de datos por medios *online* y su análisis pueda considerarse "control". El EDPB indica en la Guía que es necesario a estos efectos analizar la finalidad prevista por el responsable y, en particular, posibles tratamientos ulteriores, como el perfilado de los datos personales. Es relevante en este análisis tener en cuenta que el concepto de "dato personal" que aplican las autoridades europeas de protección de datos alcanza datos esencialmente técnicos, como la dirección IP o determinados identificadores unitarios de dispositivos, por lo que no es necesario que se recojan datos como nombre o dirección para que se considere que existe recogida y tratamiento de datos conforme al RGPD.

Para el EDPB, en particular, existirá "*control de comportamiento*" si se utilizan tecnologías como, por ejemplo, las que permiten realizar *marketing* comportamental (*behavioural advertisement*), geolocalización —sobre todo si tiene fines de *marketing*—, seguimiento *online* a través de *cookies* o tecnologías similares (p. ej., *fingerprinting*), servicios personalizados de dieta o de seguimiento de salud, videovigilancia, encuestas de mercado o estudios comportamentales basados en perfiles individuales, o la monitorización o reporte regular del estado de salud de un individuo. Muchas de estas tecnologías están ampliamente extendidas y generalizadas, tal como se establece en el apartado 2.c) de la Guía. Por ello, sería recomendable un análisis más específico por parte de la autoridades de en qué casos consideran que una organización queda sujeta al RGPD o si la mera existencia de cualquiera de estas tecnologías en servicios o aplicaciones potencialmente disponibles a interesados ubicados en la UE podría dar lugar a la aplicación del RGPD.

La determinación de los casos en los que es de aplicación el RGPD a organizaciones no europeas es una cuestión compleja, más aún cuanto más complejos se vuelven los modelos de negocio y las tecnologías aplicadas por las organizaciones. Debe

realizarse un análisis completo y detallado de los modelos de negocio, la organización de los grupos empresariales y las tecnologías concretas utilizadas. Este análisis se ha convertido en una cuestión de gran relevancia por cuanto la aplicación del RGPD implica muy diversas obligaciones, entre las que estaría la designación de un representante en la UE, numerosas medidas organizativas, así como el riesgo de sanciones significativas y los consecuentes riesgos reputacionales. Sin embargo, quedan aún algunas cuestiones pendientes de determinar por las autoridades, por lo que hacer un seguimiento de los pronunciamientos de las autoridades en los Estados miembros y de los pronunciamientos judiciales que se sucederán en casos concretos en el futuro será esencial para terminar de concretar y establecer con mayor precisión este ámbito de aplicación territorial.

Leticia López-Lapuente (*)

(*) Abogada del Área de Derecho Mercantil y Responsable de las Áreas de Protección de Datos e Internet de Uría Menéndez (Madrid).