

miembros sea de aplicación en virtud del Derecho internacional público. Esto podría incluir, por ejemplo, embajadas, consulados u oficinas de representación de la UE en terceros países, donde el tratamiento de datos personales se lleva a cabo en el marco de las actividades relacionadas con dichas representaciones. Este enfoque garantiza que la normativa europea sobre protección de datos se extienda a contextos específicos, incluso fuera de las fronteras de la UE, reforzando la protección de los derechos de los interesados.

Con este panorama normativo de aplicación extraterritorial existe el riesgo de una interpretación expansiva del mencionado 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. Este riesgo aumenta en un entorno digital globalizado donde las entidades no europeas tienen un acceso cada vez más sencillo al mercado europeo, ya sea mediante comercio electrónico, aplicaciones móviles o plataformas de redes sociales. Tal escenario plantea desafíos operativos y legales significativos para las empresas, que deben asegurarse de cumplir con los estándares europeos, aunque sus operaciones principales se realicen fuera de la UE. 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. Un ejemplo claro sería una plataforma de streaming de origen no europeo que recopile datos sobre las preferencias de visualización de usuarios europeos con el fin de personalizar recomendaciones o diseñar estrategias de marketing. Si la finalidad del tratamiento está directamente relacionada con la monitorización y el perfilado de usuarios en la UE, el RGPD podría aplicarse, obligando a la plataforma a cumplir con los requisitos establecidos en la normativa europea. 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. Esta definición amplia del término "dato personal" amplía el ámbito de aplicación del RGPD, incluyendo incluso aquellos tratamientos que, en otras jurisdicciones, podrían no considerarse como datos sensibles o protegidos. Esto implica que incluso actividades aparentemente inofensivas, como el análisis de patrones de navegación o la personalización de contenido en función de ubicaciones geográficas, pueden activar la aplicabilidad del 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. Estas actividades abarcan una amplia gama de sectores, desde el comercio minorista y los servicios financieros hasta la salud y el bienestar, lo que subraya la necesidad de que las empresas en todos los ámbitos consideren cuidadosamente cómo sus tecnologías y prácticas pueden someterlas al cumplimiento del RGPD. 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 las 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. Esta recomendación resulta especialmente relevante en un contexto donde las líneas entre lo local y lo global son cada vez más difusas. La falta de claridad podría generar una carga desproporcionada para pequeñas y medianas empresas que operan internacionalmente y no cuentan con recursos suficientes para garantizar el cumplimiento completo del RGPD.

En este contexto, especial atención merece ejemplo 13 que el EDPB plantea en su Guía:

Example 13.- *A private company based in Monaco processes personal data of its employees for the purposes of salary payment. A large number of the company's employees are French and Italian residents. In this case, while the processing carried out by the company relates to data subjects in France and Italy, it does not takes place in the context of an offer of goods or services. Indeed, human resources management, including salary payment by a third-country company cannot be considered as an offer of service within the meaning of Art 3(2)a. The processing at stake does not relate to the offer of goods or services to data subjects in the Union (nor to the monitoring of behaviour) and, as a consequence, is not subject to the provisions of the GDPR, as per Article 3. This assessment is without prejudice to the applicable law of the third country concerned”.*

Así las cosas, en la medida en que los trabajadores afectados por el tratamiento, residentes en Italia y Francia, realicen su trabajo habitualmente en Mónaco, puede entenderse el resultado alcanzado. Ahora bien, ¿si la empresa no está “based” en Mónaco sino en EEUU y tiene cientos de trabajadores residentes en la UE que prestan servicios de teletrabajo? En las situaciones típicas si tiene

cientos de trabajadores en la UE, tendrá uno o varios establecimientos en la UE, de modo que la aplicación del RGPD resultará de lo previsto en su artículo 3.1. Ahora bien, ese puede no ser el caso si todos los trabajadores residentes en la UE llevan a cabo actividades propias de teletrabajo. En un escenario como este la aplicación del criterio recogido en el ejemplo 13, y la no aplicación del RGPD puede resultar difícil de justificar^{19,20}

REFERENCIAS

Aced Félez, E. Transferencias internacionales de datos. En PIÑAR MAÑAS, J. L. (Dir.), *Protección de datos de carácter personal en Iberoamérica (II Encuentro Iberoamericano de Protección de Datos, La Antigua- Guatemala, 2-6 de junio de 2003)* (pp. 123-125). Valencia: Tirant lo Blanch, 2005.p. 123-125

BRKAN, M. Data protection and European private international law: observing a bull in a China shop. *International Data Privacy Law*, v.5, n.4, 2015.

CERVERA NAVAS, L. (2023). Cinco años de GDPR, una construcción sólida a la que se puede dotar de un poco más de flexibilidad sin comprometer sus cimientos. *Diario la ley*, 25 may.2023. <https://diariolaley.laleynext.es/dll/2023/05/25/cinco-anos-de-gdpr-una-construccion-solida-a-la-que-se-puede-dotar-de-un-poco-mas-de-flexibilidad-sin-comprometer-sus-cimientos>.

DE MIGUEL ASENSIO, P. Ámbito de aplicación territorial del Reglamento UE sobre protección de datos: casos difíciles. Pedro de Miguel Asensio,2019 <https://pedrodemiguelasensio.blogspot.com/2019/04/ambito-de-aplicacion-territorial-del.html>.

¹⁹ Vid. De Miguel Asensio, P. (2019). Ámbito de aplicación territorial del Reglamento UE sobre protección de datos: casos difíciles. Pedro de Miguel Asensio. <https://pedrodemiguelasensio.blogspot.com/2019/04/ambito-de-aplicacion-territorial-del.html>.

²⁰ No cabe desconocer que, en virtud del artículo 8 del Reglamento “Roma I”, en el marco del Reglamento “Roma I”, esos contratos de trabajo se regirán por la ley del Estado miembro de la UE en el que el trabajador realiza su trabajo o, por lo menos, el trabajador no podrá ser privado de la protección que le proporcionen las disposiciones imperativas de la ley de ese Estado miembro, en virtud de lo dispuesto en el artículo 8 del Reglamento “Roma I”. Vid. De Miguel Asensio, P. (2019). Ámbito de aplicación territorial del Reglamento UE sobre protección de datos: casos difíciles. Pedro de Miguel Asensio. <https://pedrodemiguelasensio.blogspot.com/2019/04/ambito-de-aplicacion-territorial-del.html>.

