IP, IT & Data Protection

Implementación y sanciones del RGPD

Diciembre 2019

Análisis comparado paneuropeo de infracciones y sanciones en el último año y medio

El 25 de mayo de 2018 entró en vigor el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016,

El RGPD ofrece un nuevo marco para la protección de datos, con más obligaciones para las organizaciones y un alcance territorial ampliado. El RGPD es aplicable a cualquier organización -sin prejuicio de su domicilio social, si ofrece bienes o servicios a ciudadanos que se encuentren en la UE o si se dedica a controlar el comportamiento de dichos ciudadanos en la UE.

El RGPD ha ayudado a sensibilizar a la opinión pública sobre los derechos de privacidad. Desde su entrada en vigor, más de 300.000 casos han llegado a las autoridades nacionales de protección de datos -de los cuales 150.000 provienen de quejas individuales-, se han nombrado y registrado más de 400.000 Delegados de Protección de Datos, se notificaron 90.000 violaciones de datos, y las sanciones otorgadas en toda la UE ascienden ya a millones de euros. Muchas empresas, grupos de presión e instituciones han criticado y descrito los desafíos asociados al cumplimiento del RGPD por las diversas formas en que la ley ha afectado a las empresas, la innovación digital, el mercado laboral y los consumidores.

Uno de los desafíos criticados se refiere a una supuesta falta de consistencia en su implementación en los distintos estados miembros. Por ello, en este artículo analizaremos cómo ha afectado dicho reglamento en determinados países de la Unión Europea (artículo original publicado por primera vez en mayo de 2019, actualizado posteriormente).

Los países analizados son los siguientes:

- España
- Alemania
- Austria
- Polonia
- Italia
- Hungría
- Grecia

- Rumanía
- Portugal

España

En España, desde la entrada en vigor del RGPD se han producido varios desarrollos legislativos relevantes. En diciembre de 2018 se aprobó una nueva Ley de Protección de Datos (LOPDGDD) que desarrolla ciertos aspectos del RGPD.

Durante el año 2018 el número de reclamaciones de los interesados presentadas ante la Agencia Española de Protección de Datos (en adelante, "**AEPD**") se ha incrementado un 33% respecto al año anterior. Para el año 2019 se espera un crecimiento similar.

La implicación de la AEPD en tareas de sensibilización, orientación y apoyo a la implementación de la RGPD ha sido enorme y se han publicado varias herramientas de apoyo y directrices.

Si bien en los primeros meses posteriores a la entrada en vigor del RGPD la AEPD se ha centrado principalmente en el análisis de infracciones y en el envío de advertencias a numerosas empresas, al cabo de un tiempo comenzaron a publicarse sanciones específicas, con un total de 15 sancines publicadas hasta finales de 2019.

La sanción más elevada hasta el momento ha sido una por 250.000 euros, impuesta a "La Liga", una aplicación que utilizaba la geolocalización y el micrófono del teléfono móvil de millones de usuarios a fin de combatir la piratería en establecimientos públicos que emitían partidos de fútbol sin licencia. Según la AEPD, esta aplicación no cumplía los requisitos de transparencia relativos al tratamiento, y tampoco permitía a los usuarios revocar el consentimiento.

En cuanto a los apercibimientos que ha realizado la AEPD, destaca el caso de dos resoluciones similares, pero no idénticas, relativas a dos colegios y a los datos personales y fotos de los alumnos, en las que la AEPD tuvo en cuenta los esfuerzos desplegados por ambas escuelas en las medidas de protección de datos adoptadas tanto antes como después de que se produjera la infracción de protección de datos. Es de esperar, no obstante, que se hagan públicas en las próximas semanas o meses más sanciones. Así lo ha declarado públicamente en varios medios la directora de la propia AEPD.

Otras sanciones importantes publicadas incluyen compañías de distintos sectores:

- Dos compañías telefónicas fueron multadas con 60.000 y 36.000 euros, respectivamente, por falta de base jurídica en sus tratamientos. En el primer caso, se usó información personal sin consentimiento para la celebración de contratos telefónicos; en otro caso, la compañía

continuó tratando información personal incluso cuando los sujetos aludidos solicitaron el fin de estas prácticas.

- Una empresa de cosméticos fue sancionada con una multa que ascendió hasta 60.000 euros por un proceso de verificación de identidad personal erróneo por el que un usuario fue incluido en un registro de morosos impidiendo que operara normalmente con su banco habitual.

- Una aerolínea fue multada con 30.000 euros ya que no era posible rechazar las *cookies* de su página web y que el usuario pudiera continuar navegando en la misma.

- Una empresa de cobro de deudas fue sancionada con una multa de 60.000 euro por tener una base legal insuficiente con relación al tratamiento de datos. Concretamente, un usuario que supuestamente no devolvió un microcrédito comenzó a recibir mensajes de reclamación , no solo en su dirección de correo personal, sino en una dirección de correo de su puesto de trabajo, que además era accesible para el personal de toda la oficina. Dicha dirección de correo no había sido facilitada por el mismo.

Otras sanciones menores han sido impuestas a compañías de gas, juego online, operadores eléctricos, incluso a algunas PYMES; multas que han oscilado entre los 1.000 y los 12.000 euros.

Alemania

Desde la entrada en vigor del RGPD en mayo de 2018, las autoridades alemanas de protección de datos han impuesto 75 sanciones en esta materia.

Se publicó recientemente que la multa más alta en un solo caso en Alemania fue de aproximadamente 14,5 millones de euros y se impuso contra una empresa inmobiliaria (Deutsche Wohnen SE). La compañía había recopilado y almacenado una gran cantidad de datos personales de sus inquilinos en un sistema de archivo durante años sin verificar si ello era necesario y legalmente permitido. Una primera queja de la autoridad de protección de datos en 2017 había sido ignorada. Sin embargo, la decisión aún no es definitiva, ya que Deutsche Wohnen podría apelar la multa.

Al igual que Deutsche Wohnen SE, una empresa de entrega de alimentos recibió una multa de aproximadamente 200.000 euros por no eliminar las cuentas de antiguos clientes en diez casos, a pesar de que esos sujetos de datos no habían estado activos en la plataforma de servicios de entrega de la compañía durante años. En otro caso, la autoridad de protección de datos de Berlín impuso una multa de 50.000 euros a un banco que había tratado datos no autorizados de antiguos clientes. Una red social

alemana tuvo que pagar una multa de 20.000 euros por almacenar datos de usuarios sin cifrar en servidores antiguos..

Algunas autoridades alemanas de protección de datos ya han dejado claro que realizarán inspecciones sin previo aviso y que aumentarán el número de empleados.

En consecuencia, la concienciación sobre la protección de datos ha aumentado considerablemente en Alemania. Las empresas han "ordenado" sus bases de datos, han obtenido una visión general de sus procesos de protección de datos y han ajustado los mismos para cumplir con los requisitos del RGPD.

Sin embargo, las pequeñas empresas y asociaciones alemanas han manifestado quejas debido al alto nivel de burocracia que implican las obligaciones de información y documentación. El Comisario Federal de Protección de Datos de Alemania ha considerado en su informe anual reducir los gastos burocráticos de las pequeñas empresas y asociaciones.

Austria

Desde la entrada en vigor del RGPD en Austria se han producido cambios notables, aunque no dramáticos: el número de reclamaciones aumentó rápidamente entre 2017 y 2018, triplicándose. Sin embargo, la sanción más alta en este periodo sigue siendo bastante moderada, ascendiendo a un total de 4.800 euros.

Poco a poco, y a pesar de que estas sanciones todavía son manejables, se observa un cambio en la jurisdicción de la Autoridad de Protección de Datos. Los requisitos de la Autoridad de Protección de Datos para con los responsables de tratamiento han aumentado notablemente, especialmente en lo que respecta a las medidas de seguridad (especialmente en el sector de la asistencia sanitaria), así como a los requisitos de información y a los requisitos formales de consentimiento y de grabación de vídeo. En la práctica, cientos de consentimientos inválidos pueden ser comercialmente más dañinos que una multa, ya que los datos pertinentes ya no pueden utilizarse legalmente y pueden producirse reclamaciones por daños y perjuicios. Según lo que muestran las decisiones actuales, no se debería confiar en la hasta ahora práctica de "consulta en lugar de sanción" prometida inicialmente por los políticos en Austria. Al menos ahora, todo el mundo debería cumplir con el RGPD.

Por eso, y durante 2019, los procedimientos ante la Autoridad de Protección de Datos han aumentado considerablemente – y en consecuencia las multas–. Durante este año, un centro de alergias fue multado con 50.000 euros por incumplimiento con las normas de información a los usuarios y por no nombrar un Delegado de Protección de Datos a pesar de la obligatoriedad de ello. Un entrenador de futbol fue multado por grabar a sus jugadoras en las duchas. Aunque esto no fue considerado como un

crimen (se retiraron los cargos penales), se le fue impuesta una multa de 11.000 euros por violación de la privacidad.

Por remarcar algún aspecto, es interesante la sentencia de la Autoridad de Protección de Datos en la que aclara que anonimizar es un modo legítimo de cumplir con la obligación de eliminar alguna información referente a personas. Esta sentencia emanó de un caso en el que una página web de *reviews* de doctores médicos, donde el interés y el derecho a tener información de los potenciales clientes prevaleció sobre la voluntad de los doctores de no ser incluidos en dicho portal.

Polonia

Desde que el RGPD entró en vigor, se ha apreciado una intensificación de los esfuerzos de la Autoridad de Supervisión Polaca (en adelante, "**PUODO**"). A lo largo de este período, la PUODO ha proporcionado una amplia orientación y ha anunciado un plan de inspecciones para 2019. El plan involucra principalmente a entidades públicas, el sector financiero y empresas dedicadas al telemarketing. La PUODO ha declarado prestar especial atención a la videovigilancia y a la contratación de personal.

Hasta ahora se han impuesto tres multas administrativas en Polonia. La primera, de casi un millón de PLN (unos 230.000 euros), se impuso a una empresa que utilizaba datos personales de empresarios en su actividad empresarial. Los datos fueron recogidos y presentados en la página web de la empresa, sin que los interesados hubieran sido informados de ello en la forma exigida por el artículo 14 del RGPD. El segundo caso se refería a una asociación regional de fútbol que publicó en su sitio web los nombres, direcciones y números de identificación personal de 585 árbitros. La multa fue de 55.000 PLN (unos 13.000 euros) y se redujo gracias a la buena cooperación, al cumplimiento de las instrucciones de la PUODO y al hecho de que ninguno de los árbitros sufrió daños.

La tercera y más reciente sanción ascendió hasta casi 3 millones de PLN (cerca de 660.000 euros). Fue impuesta el 10 de septiembre y publicada el 19 de ese mes. La multa fue impuesta a una reconocida tienda online de electrónica, la cual no había asegurado la debida protección de la información de carácter personal que registraba. Se produjo una fuga de datos debido a un ataque informático por el cual se filtró la información personal de cerca de 2,2 millones de personas. Probablemente, toda esta información fue vendida en la *Darknet*. Además, los datos filtrados de 35.000 clientes de esta tienda online eran de carácter económico ya que algunas de las transacciones que se realizaban en esta plataforma eran de alquiler. Esta información robada fue para *phishing* o para enviar mensajes amenazantes solicitando dinero. Esto fue considerado por la PUODO como una violación de los derechos y libertades de los usuarios. La tienda online penalizada informó de que iba a apelar.

Estas no fueron las únicas infracciones detectadas por el órgano de vigilancia, pero las demás infracciones no fueron sancionadas.

El RGPD suscitó gran preocupación entre los empresarios polacos en mayo de 2018. Sin embargo, también provocó un aumento considerable de la concienciación sobre la protección de datos personales. Además, el RGPD influyó positivamente en algunas PYMES polacas, que ahora realizan tratamiento de datos con mayor cuidado y se esfuerzan por garantizar su cumplimiento.

El RGPD tiene algunos efectos secundarios en Polonia, siendo uno de ellos el llamado "troleo RGPD", según el cual se envía *spam* a empresas polacas con solicitudes de datos personales, con la esperanza de descubrir alguna infracción para poder así reclamar daños y perjuicios. Hasta ahora parece que estos intentos han resultado inútiles.

Italia

En Italia han pasado pocos días desde el inicio de la plena aplicación del nuevo régimen de sanciones previsto por RGPD.

Aunque el RGPD entró en vigor el 25 de mayo de 2018, Italia estableció un "período de gracia", mediante el artículo 22, apartado 13, del Decreto Legislativo 101/2018, según el cual, durante los primeros ocho meses, a partir de septiembre de 2018, la Autoridad Italiana de Protección de Datos no impondría ninguna sanción relacionada con el RGPD. Este periodo finalizó el 19 de mayo.

Durante 2018, la Autoridad Italiana de Protección de Datos se centró en cuestiones relacionadas con el software malicioso, aspectos del derecho laboral, la ciberseguridad, la asistencia sanitaria, la facturación electrónica y el telemarketing, como subrayó el presidente de la Autoridad durante el informe de actividad de 2018.

Durante 2019, la Autoridad Italiana de Protección de Datos ha acogido varios asuntos relacionados con el "derecho al olvido". En uno de estos, la Autoridad reconoció el derecho "a ser olvidado" de una persona que había estado en rehabilitación criminal, considerando a su favor el tiempo desde que se cometió el crimen, así como el desproporcionado impacto negativo derivado de la persistencia de esta información criminal en Internet.

Además, la Autoridad Italiana de Protección de Datos ha emitido muchas declaraciones sobre la violación de datos personales. En relación con el artículo 28(2) punto (e) del RGPD, la Autoridad ordenó a un servidor de correo electrónico volver a ponerse en contacto con los usuarios que se vieron afectados por una fuga de información personal debido a una conexión Wi-Fi fraudulenta y que causó la filtración de datos personales de casi un millón y medio de usuarios. Esto se debe a que la primera vez que la

compañía se puso en contacto con los usuarios afectados no cumplió con lo establecido en el artículo 34(2) del RGPD, además también se consideró que esta comunicación fue enviada a los correos electrónicos cuyas credenciales habían sido filtradas.

Con relación a los casos de violación de datos, el 30 de julio de 2019, la Autoridad Italiana de Protección de Datos puso a disposición del público un formulario de notificación para estos casos donde se violó algún tipo de información personal.

Hungría

Desde la entrada en vigor del RGPD, la Autoridad Húngara de Protección de Datos (NAIH) ha impuesto multas administrativas de entre 100.000 y 11.000.000 HUF (unos 300 y 34.000 euros); en una ocasión, impuso una multa de 30.000.000 HUF (unos 91.000 euros).

La NAIH ha impuesto multas notables a compañías privadas, pero también a organizaciones públicas. Por ejemplo, multó con una cuantía de 5.000.000 HUF (unos 15.000 euros) a la policía por no notificar la pérdida de un *pendrive* que contenía información personal de 1.733 empleados; y 3.000.000 HUF (unos 9.000 euros) a un Tribunal de Justicia por recoger las afiliaciones de alguno de sus jueces.

La multa administrativa más severa fue impuesta a la empresa organizadora de un reconocido festival. Esta multa ascendió hasta 30.000.000 (unos 91.000 euros). En este caso, la NAIH encontró almacenada más información de carácter personal de la necesaria para los objetivos perseguidos: los carnés de identidad de los visitantes habían sido escaneados y la información de estos carnés había sido vinculada a las entradas al festival como condición para acceder al área donde se celebra el mismo, con la intención de prevenir ataques criminales, terroristas o incluso la reventa de entradas. Sin embargo, la NAIH declaró que para conseguir estos propósitos se habían realizado actividades poco prácticas y no del todo aceptadas por el RGPD. La multa ascendió hasta el 2,4% de la facturación anual de la empresa en cuestión.

Como tendencia general, la NAIH parece aplicar las bases legales del RGPD de una manera estricta y restrictiva. Además, las sanciones impuestas por la NAIH están basadas en los intereses legítimos, considerándose necesario la presencia de pruebas debidamente documentadas y razonadas, de lo contrario, el NAIH desestima el proceso por no tener una base legal suficiente.

Grecia

Durante los primeros meses, la autoridad griega de protección de datos ha dictado un número poco relevante de decisiones en relación con el RGPD. En tales decisiones, la autoridad ha sido más bien indulgente, ya que ha optado por apercibir a los responsables del tratamiento en lugar de imponer sanciones.

En algunos casos de incumplimiento de la obligación de notificación de la violación de datos personales, la Autoridad Griega de Protección de Datos emitió una amonestación, teniendo en cuenta que: a) el RGPD acababa de empezar a aplicarse; b) los responsables del tratamiento reaccionaron inmediata y con rapidez y trataron eficazmente la violación de datos; c) la violación de datos se refería a un número muy limitado de personas físicas; d) el ciberataque denunciado en uno de los casos era desconocido y muy complejo.

En el único caso relativo al incumplimiento de las obligaciones relativas a comunicaciones publicitarias no solicitadas, la Autoridad optó por una amonestación ya que se trataba de una sola persona física que se quejaba de haber recibido mensajes publicitarios a través de la aplicación Viber sin haber dado su consentimiento de conformidad con las disposiciones pertinentes del RGPD. Es fundamental, en opinión de la Autoridad, proporcionar suficiente información a la persona física y declarar claramente la finalidad del tratamiento, es decir, si éste se enmarca en el contexto del contrato o si es de carácter promocional.

Cabe señalar que, en los casos decididos en el marco legislativo anterior, la Autoridad parece haber endurecido su postura y, en algunos casos, ha impuesto multas que alcanzan el límite máximo de 150.000 euros.

Sin embargo, la Autoridad ha impuesto recientemente dos sanciones de 400.000 euros a un servidor de comunicación electrónica. Las multas fueron impuestas, en el primer caso debido a que el Delegado de Protección de Datos conservó los datos personales de los suscriptores más tiempo del permitido. En el segundo caso, debido al incumplimiento del derecho de los interesados a objetar.

Estas dos sanciones son bastante significativas en la era posterior a la aplicación del RGPD.

En el primer caso, se debió a un error en los registros de aquellos suscriptores que habían ejercido previamente su derecho a no ser incluidas entre los destinatarios de las llamadas con fines promocionales. Debido a una mala actualización de estas bases de datos y a un error técnico, usuarios que habían ejercido este derecho recibieron llamadas promocionales repetidas veces.

En el segundo caso, debido a un error técnico, los destinatarios de mensajes promocionales no tenían la opción de causar baja de estos servicios, menester obligatorio mediante un enlace que debe posicionarse en dichos los mensajes promocionales. Como enfatizó posteriormente la Autoridad de

Protección de Datos, no solo se incumplió el derecho, sino que tampoco se implementó una medida adecuada que permitiera detectar esta infracción.

Varias circunstancias fueron consideradas como factores agravantes y atenuantes, respectivamente. Por ejemplo, la cantidad de usuarios afectados, la duración del incumplimiento, la actividad principal de la compañía en cuestión, la responsabilidad de esta en un incidente de violación de datos anterior y una antigua "advertencia" por parte de la Autoridad con este respecto, fueron considerados como factores agravantes. Sin embargo, la falta de intención, las medidas correctivas adoptadas y la cooperación con la Autoridad también fueron consideraros como factores atenuantes.

El principio de protección de datos se establece a través de decisiones de una gran importancia. Este principio no constituye un requisito teórico, sino que es necesidad práctica y actual para las empresas. Esta decisión hace eco de la creciente necesidad de auditorías internas para identificar brechas de seguridad y salvaguardar la información personal, tanto a la hora de determinar qué medios son los adecuados para procesar esta información, como para establecer las medidas necesarias a la hora de procesar esta información. Auditorías internas e implementación de técnicas adicionales y medidas organizativas. Si las compañías no adoptan estas medidas en pro del RGPD, es muy posible que tengan que enfrentarse a las sanciones pertinentes por parte de las autoridades competentes.

Además, la autoridad ha anunciado que ha llevado a cabo más de 65 investigaciones a distancia autoiniciadas en las páginas web de empresas de diversos sectores de la economía, con el fin de controlar el cumplimiento de una serie de obligaciones en virtud de la RGPD. La autoridad ha enviado notificaciones a los responsables del tratamiento, ordenándoles que ajusten las operaciones de tratamiento a las disposiciones de la RGPD en un plazo determinado, en algunos casos mediante la adopción de determinadas medidas específicas propuestas por la Autoridad, y que le informen al respecto.

Además, la Autoridad ha publicado la lista de actividades de tratamiento de datos que, en su opinión, deben estar cubiertas por una evaluación del impacto de protección de los datos.

Asimismo, es interesante mencionar que la autoridad ha anunciado que ha recibido desde el 25 de mayo de 2018 hasta principios de este año más de 96.000 quejas de los titulares de los datos alegando infracción de las disposiciones de RGPD. Queda por ver qué parte de ellas está justificada y, como tal, dará lugar a la adopción de medidas sancionadoras significativas por parte de la Autoridad de Protección de Datos.

Por último, cabe señalar que Grecia todavía no ha adoptado legislación para cubrir las áreas que se dejan a la jurisdicción de los Estados miembros.

Rumanía

Desde la entrada en vigor del RGPD, se han producido algunos avances notables en materia de protección de datos en Rumanía. En 2018 el Parlamento aprobó la Ley nº 190 que aborda algunos de aspectos del RGPD. Además, al mismo tiempo, las Directivas 2016/680 y 2016/1148 han sido transpuestas a la legislación nacional.

En cuanto a la legislación de desarrollo y las guías de mejores prácticas, la actividasd de la Autoridad de Protección de Datos es bastante escasa. Algunas asociaciones profesionales que representan a responsables de tratamiento en sectores como la banca, las telecomunicaciones o la edición, han presentado códigos de conducta para su aprobación por parte de las Autoridades de Protección de Datos, pero, según nuestra información , ninguno de estos códigos ha sido aprobado todavía por las Autoridades de Protección de Datos. En lugar de ello, el Delegado Protección de Datos ha optado por concentarse en crear concienciación a nivel informal, participando en muchas conferencias y eventos locales dedicados al RGPD, organizados tanto por el sector público como por el privado.

Durante el primer año de vigencia del RGPD, se han registrado 5.260 quejas (el doble que el año anterior) y 400 incidencias referidas a violaciones de datos. Durante el primer año de esta legislación, la Autoridad de Protección de Datos ha abierto 496 investigaciones conforme a quejas, mientras que casi el mismo número de investigaciones (concretamente 485) han sido abiertas *ex oficio*.

En relación con las sanciones impuestas, la más alta (actualmente la segunda más alta en Europa Central) fue al sector bancario. En concreto, un banco no adoptó las medidas técnicas y organizativas apropiadas para garantizar el cumplimiento del principio de minimización de datos y el principio de protección de datos. Este fallo produjo que documentos con información financiera fuera puesta a disposición de terceros en la nube, revelando los carnés de identidad y las direcciones de más de 300.000 usuarios con cuentas operativas en este banco.

En otro caso, un hotel tuvo que hacer frente a una sanción de 15.000 euros por no aplicar las medidas técnicas y organizativas apropiadas (concretamente, las medidas para supervisar que la información era conservada de manera confidencial). Este hecho terminó con la revelación en la nube de nombres y preferencias alimentarias de 46 usuarios.

Otra sanción de 3.000 euros fue impuesta a un sitio web de mensajería instantánea, debido a una mala gestión de la migración entre plataformas de información de carácter personal, lo que confirió acceso público a información como nombres, apellidos, números de teléfonos, direcciones, lugares de trabajo y detalles de transacciones, a través de varios *links*.

Otra organización fue multada con 2.500 euros por (i) no ser capaz de probar que sus empelados estaban bien informados sobre el uso de un CCTV de un sistema de vigilancia, y (ii) por hacer público en su tablón de noticias los números de identidad de algunos de sus empleados.

La Autoridad de Protección de Datos Rumana (ANSPDCP) impuso una sanción al Raiffeisen Bank y a un corredor de bolsa (Vreau Credit S.R.L.), de 150.000 euros y 20.000 euros respectivamente.

En el primer caso, el banco fue sancionado por no adoptar las medidas técnicas y organizativas necesarias para prevenir el acceso de terceras personas y filtraciones de información de carácter personal. Dos empleados del banco solicitaron a la Agencia de Crédito Nacional información de 1.177 clientes. El corredor de bolsa envió los carnés de identificación a empleados del Raiffeisen Bank vía WhatsApp. Además, los mismos empleados del banco solicitaron a la Autoridad Nacional Fiscal (ANAF) la información de 124 clientes del corredor de bolsa y estos se la enviaron. El banco notificó de esta fuga de información al ANSPDCP. Aun así, el banco fue sancionado por no asegurar que sus empleados pudieran acceder únicamente a la información que responde a su posición y sus obligaciones. El Broker que había solicitado dichos datos fue multado por divulgar la identidad de sus clientes y por no informar debidamente sobre esta filtración al ANSPDCP.

Portugal

Una de las primeras sanciones impuestas tras la entrada en vigor del RGPD fue al Hospital de Barreiro, uno de los hospitales públicos más reconocidos de la región de Lisboa. La infracción se refería al acceso indiscriminado a datos clínicos. La sanción se basaba en las siguientes infracciones del RGPD: el principio de minimización de datos, ya que el Hospital permitió el acceso indiscriminado a un conjunto excesivo de datos a profesionales que sólo podían acceder a ellos en casos previamente justificados; los principios de integridad y confidencialidad, por no aplicar medidas organizativas y técnicas destinadas a impedir el acceso ilícito a los datos personales; la incapacidad del Hospital para garantizar la integridad, confidencialidad, disponibilidad y resiliencia permanente de los sistemas y servicios de tratamiento y la falta de aplicación de medidas organizativas y técnicas adecuadas para garantizar un nivel de seguridad adecuado al riesgo, en particular, un proceso para poner a prueba, evaluar y evaluar periódicamente la eficacia de las medidas de seguridad del tratamiento de los datos. La Autoridad de Protección de Datos Portuguesa (CNPD) impuso al Hospital de Barreiro una sanción de 400.000 euros.

Además del caso del Hospital de Barreiro, la Autoridad Portuguesa de Protección de Datos ha emitido durante 2019 nuevas sanciones en entidades privadas. Sin embargo, la CNPD decidió no hacer pública la identidad de dichas compañías. La más alta alcanzó la cantidad de 20.000 euros, y fue debida a la violación del derecho de los usuarios de acceso a sus datos. En los otros dos casos, la CNPD impuso multas de 2.000 euros debido a violaciones del artículo 13/1 y 2 del RGPD (información que debe

proporcionarse cuando se recopilan datos personales del interesado), en relación con el uso de videovigilancia.

Por otro lado, este año, el Parlamento se ha visto sometido a una "frenética producción de conducta legislativa" en lo referido a Protección de Datos. En nuestra opinión, se ha generado un "enredo" regulatorio e institucional. El pasado junio, el Parlamento aprobó cuatro nuevas leyes en protección de datos, entre ellas la nueva ley que implementa el RGPD y la nueva ley que desarrolla el RGPD solo para el sistema judicial, con otra Autoridad de Protección de Datos. Además, las directivas 2016/680 y 2016/1148 se han transpuesto en la legislación nacional.

Aun así, la implementación del RGPD únicamente en sistemas judiciales fue vetada por el presidente de la República. Esta nueva ley asigna a los magistrados judiciales y al MP la responsabilidad del tratamiento de datos en los procesos de su competencia y crea una nueva Autoridad de Protección de Datos cuya composición (ministerial) es impugnada y es probable, según nuestro parecer, que viole el principio de separación de poderes.

Respecto a esta ley, y a través de deliberación, el CNPD decidió no aplicar quince artículos de la ley que implementa el RGPD. La CNPD justifica que esos artículos no cumplen con la RGPD.

En los últimos meses, la CNPD ha publicado dos comunicados. En primer lugar, considera que la lista de actividades de tratamiento de datos que deben estar cubiertas por un Delegado de Protección de Datos. Por otro lado, la Autoridad de Protección de Datos portuguesa también emitióuna deliberación interpretativa sobre la posibilidad de que las autoridades estén exentas de multas, previstas por la nueva ley, durante los próximos tres años. Esto se debe a que varias entidades públicas han solicitado esta exención, la CNPD decidió que solo puede decidirla, *in casu*.

Andersen Tax & Legal | Service Line IP, IT & Data Protection

Artículo en colaboración. Agradecimientos:

> España · Belén Arribas · belen.arribas@AndersenTaxLegal.es
> Alemania · Dr. Fritjof Börner · fritjof.boerner@AndersenTaxLegal.de
> Polonia · Magdalena Patryas · magdalena.patryas@andersentaxlegal.pl
> Italia · Francesco Inturri · francesco.inturri@andersentaxlegal.it
> Hungría · Tamás Szabó · tamas.szabo@sz-k-t.hu
> Hungría · Tamás Kárpáthegyi · tamas.karpathegyi@sz-k-t.hu
> Grecia · Dr. Themistoklis K. Giannakopoulos · themistoklis.giannakopoulos@AndersenLegal.gr
> Rumanía · Bogdan Halcu · bogdan.halcu@tuca.ro
> Austria · Katharina Raabe-Stuppnig · raabe@lansky.at
> Portugal · Raquel Brízida Castro · raquel.castro@AndersenTaxLegal.pt