DATOS Opinión

Sin datos no hay culpable: cómo se preparan las empresas para investigaciones internas transfronterizas

ANDREA SÁNCHEZ / JONATHAN GÓMEZ PÉREZ-LLORCA

17 JUL. 2020 - 07:26

Cumplidos dos años desde la entrada en vigor del Reglamento General de Protección de Datos, no son pocas las organizaciones que continúan adaptando sus políticas y procedimientos internos a la nueva regulación.

El esfuerzo realizado por las empresas en términos de *compliance* ha sido mayúsculo. Sin embargo, aunque numerosos profesionales han advertido del impacto del Reglamento General de Protección de Datos (RGPD) en las investigaciones internas corporativas y de la necesidad de planificarlas adecuadamente, la práctica demuestra que esta cuestión a menudo se deja a un lado cuando se trata de investigar.

Uno de los puntos más conflictivos es la gestión de las transferencias internacionales de datos. En este mundo global, cada vez son más las investigaciones internas que exigen la transmisión de datos personales a jurisdicciones externas al Espacio Económico Europeo (EEE), ya sea dentro del mismo grupo empresarial o a un tercero ajeno al mismo.

Con carácter general, los datos pueden ser transferidos a un tercer país u organización internacional, siempre que la Comisión Europea (CE) haya constatado que ofrece un nivel de protección adecuado (como es el caso de Andorra, Argentina, Guernsey, Isla de Man, Islas Feroe, Israel, Jersey, Nueva Zelanda, Suiza, Uruguay y, parcialmente, Canadá y Japón). Si el tercer país no se encuentra entre ellos, los datos sólo podrán transferirse si este hubiera ofrecido garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas, mediante la firma de normas corporativas vinculantes (BCR), la suscripción de cláusulas contractuales tipo aprobadas por la CE (SCC) o por una autoridad de control o la adhesión a códigos de conducta o mecanismos de certificación.

A falta de estas garantías, el RGPD contempla determinados supuestos en los que se permiten, de manera puntual, estas transferencias, entre los que destacan la existencia de consentimiento del interesado, la formulación de reclamaciones o la celebración de contratos.

De entre todas las garantías citadas, la suscripción de SCC es probablemente la más común para transferencias de datos intragrupo o con un tercero involucrado en la investigación. Junto a ellas, las BCR -que pueden definirse como políticas desarrolladas e implementadas dentro de un grupo empresarial con la finalidad de facilitar las transferencias internacionales de datos- son las que ofrecen mayores posibilidades en el marco de las investigaciones internas, por su versatilidad y por ajustarse mejor a las necesidades de cada organización. Ahora bien, conforme al RGPD, las BCR deben ser aprobadas por la autoridad de control competente en cada país del EEE.

En la práctica, el procedimiento de aprobación de las BCR es largo y, en ocasiones, costoso. A título ilustrativo, la AEPD aprobó las primeras BCR en el marco del RGPD el pasado mes de marzo, siendo una de las primeras que se aprobaban a nivel europeo. Es por ello que resulta de especial utilidad que las organizaciones se anticipen, tengan sus canales de transmisión de datos preparados y específicamente prevean en sus BCRs la transmisión de datos personales recabados en el marco de investigaciones internas como una categoría concreta, con un tipo de tratamiento y unos fines determinados.

Junto al cumplimiento de los requisitos descritos para transferir datos fuera del EEE, ha de garantizarse la propia seguridad de los datos a transferir en el marco de la investigación, dado que un uso indebido podría llegar a comprometer su buen fin (piénsese, por ejemplo, en datos bancarios que puedan facilitar la comisión de un fraude o datos que puedan revelar la identidad de un denunciante). El RGPD no define qué medidas de seguridad deben implementarse, de manera que es cada organización la que debe fijarlas en función de sus características, circunstancias y riesgos detectados.

En cualquier caso, la práctica forense aconseja que las medidas de seguridad sean adecuadas no sólo para prevenir ciberataques externos, sino también para controlar el acceso a los datos y garantizar la confidencialidad, integridad y disponibilidad de la información en los sistemas. Igualmente, la seudonimización y el cifrado de los datos, referidas en el RGPD, son altamente recomendables.

En definitiva, en relación con las transferencias internacionales de datos en este contexto, no existe una suerte de combinación ganadora que garantice un nivel de protección y seguridad adecuado en todas las organizaciones. Son precisamente estas las que deben analizar sus riesgos y, a partir de esta evaluación, desarrollar e implementar políticas y protocolos que se ajusten a sus necesidades y que faciliten el curso de las investigaciones. Todo ello sin perder de vista las perspectivas de futuro apuntadas por la CE en materia de desarrollo de instrumentos modernos para favorecer las transferencias internacionales de datos en su reciente informe, de 24 de junio, sobre la evaluación y revisión del RGPD.