Resolución AEPD 00677/2022: Incumplimiento del principio legitimación, privacidad desde el diseño y por defecto, y de la seguridad del tratamiento[1]

Fecha: 25 de octubre de 2023

El objeto de la presente nota es el análisis de los criterios jurídicos apreciados por la Agencia Española de Protección de Datos (en adelante, "**AEPD**" o la "**Agencia**") en la Resolución del Procedimiento Sancionador 00677/2022, de fecha 20 de octubre de 2023, la cual impone una **sanción de 1,64 millones de Euros por infracción de los artículos 6, 25 y 32 del Reglamento General de Protección de Datos (RGPD)** – 70.000 Euros por la contratación no autorizada de productos, 70.000 Euros por la incorporación de datos personales en los sistemas de información crediticia de forma ilegítima, 500.000 euros por falta de medidas de seguridad en relación con procedimientos de inclusión en sistemas de información crediticia, 500.000 Euros por el incumplimiento del principio de privacidad desde el diseño y por defecto, y 500.000 Euros por la falta de medidas de seguridad en relación con los procedimientos de contratación de productos financieros–, a la entidad financiera BANCO BILBAO VIZCAYA ARGENTARIA, S.A. (en adelante, "**BBVA**").

I. Supuesto de hecho

La AEPD admitió a trámite la reclamación presentada por un cliente de BBVA, que fue víctima de un robo de, entre otras cosas, el teléfono móvil, el documento nacional de identidad y una tarjeta de crédito. Desde ese momento, se iniciaron contrataciones de productos financieros firmados electrónicamente. La reclamante, al percatarse de la sustracción, solicita el bloqueo de sus tarjetas y lo comunica a la entidad. A pesar de la orden de paralización total y del conocimiento por parte de la entidad de la existencia de una suplantación de identidad, se permite la contratación de productos utilizando el sistema de doble factor de autenticación vía teléfono móvil durante un periodo aproximado de dos semanas. Asimismo, la reclamante es incluida en un fichero de información crediticia como consecuencia de los productos contratados suplantando su identidad.

II. Análisis jurídico

La entidad acepta la responsabilidad en la vulneración del artículo 6.1 del RGPD puesto que los productos han sido contratados por un tercero que ha sustraído los datos personales del reclamante, además del móvil como herramienta de doble factor de autenticación, incluso posteriormente de que la entidad manifestase conocer la suplantación de identidad.

A su vez, también asume la vulneración del artículo 6.1 del RGPD con relación a la incorporación de datos personales en los sistemas de información crediticia y del artículo 32 del RGPD por la falta de medidas de seguridad con relación a los procedimientos de

[1] https://www.aepd.es/documento/ps-00677-2022.pdf

comunicación, inclusión y mantenimiento en los sistemas de información crediticia de datos personales. En este caso, **la AEPD considera que BBVA no dispone de un procedimiento adecuado referido a la implementación y aplicación de medidas de seguridad de datos personales apropiadas**, técnicas u organizativas**, para evitar la inclusión o el mantenimiento de los datos de los clientes en sistemas de información crediticia** cuando la deuda es controvertida, llevando a cabo un tratamiento de datos personales sin base de legitimación alguna.

A. Sobre el cumplimiento del principio de protección de datos desde el diseño (artículo 25 RGPD).

La AEPD ha concluido que BBVA no cumplió con el principio de privacidad desde el diseño y por defecto por diversas razones:

- **El procedimiento establecido por la entidad respecto a la gestión de incidentes en relación con el fraude se encuentra totalmente desactualizado al ser elaborado en 2015**. Así, el procedimiento no se encuentra adaptado al RGPD al igual que tampoco se enfoca desde los riesgos para los derechos y libertades de los clientes, sino desde los riesgos que puede soportar la entidad.

- En este sentido, la AEPD concluye que los restantes procedimientos presentados por BBVA no recogen de forma específica el supuesto de hecho, el riesgo no se enfoca desde los riesgos en materia de protección de datos y no se traducen en una serie de medidas concretas aplicable, quedándose en directrices superficiales. Tampoco se ha realizado el pertinente análisis de riesgos, determinando las medidas técnicas y organizativas pertinentes para garantizar el respeto de los derechos de los interesados en estos supuestos.

- En consecuencia, pese a haber notificado a BBVA la sustracción del teléfono móvil y la documentación identificativa de la parte reclamante, la entidad mantuvo este dato personal de la parte reclamante como medio a través del cual se producía la autenticación de la identidad de la parte reclamante, lo que evidencia una falta de diseño de medidas adecuadas aplicables a estas situaciones.

B. Sobre la vulneración del artículo 32 del RGPD por con la falta de medidas de seguridad en relación con los procedimientos de contratación de productos financieros.

La AEPD fundamenta la vulneración de la obligación de implementar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo en varios aspectos:

- Pese a que la parte reclamante pone en conocimiento a través de los diversos canales la sustracción sufrida y las diversas operaciones fraudulentes realizadas por terceras personas no autorizadas, BBVA no impidió que se siguieran realizando operaciones ilegales con los datos personales de sus clientes, lo que pone de manifiesto la ausencia de medidas de seguridad implementadas que eviten que, comunicada por un cliente la sustracción de información, impidan que se sigan haciendo tratamientos ilegales de sus datos personales.

- Si bien BBVA alega que el acceso por el cliente a la banca on-line de BBVA exige la utilización de un primer factor de autenticación cuya custodia y control no le corresponde (sino que es una cuestión que depende del propio usuario), la AEPD considera que esto no es óbice para que la entidad aporte soluciones al cliente en caso de que un tercero tenga acceso al primer factor de autenticación, más cuando es evidente que esto se ha producido, y el cliente avisa con carácter previo que ha perdido el control sobre sus datos personales.

En este sentido, la AEPD considera que la responsabilidad recae desde el momento en que BBVA carece de medida de seguridad alguna de gestión de contraseñas, autenticación de los usuarios, de bloqueo o de algún otro tipo para evitar accesos no autorizados en supuestos de pérdida o robo de datos que pueden ser utilizados para cometer un fraude, ni siquiera para evitar que el fraude continúe cometiéndose, una vez que la pérdida o robo les ha sido comunicada.

III. Conclusión

En definitiva, sin perjuicio de otras particularidades indicadas por la AEPD en este procedimiento, relacionadas con el principio *non bis in idem*, concurso medial de conductas imputadas o el principio de proporcionalidad, **cabe destacar específicamente cómo la AEPD define el efectivo cumplimiento del principio de privacidad desde el diseño y por defecto y la obligación de implementar y aplicar medidas de seguridad conforme al artículo 32 del Reglamento, además de delimitar e individualizar ambas infracciones**.

En este sentido, los procedimientos deben recoger de forma específica los supuestos de riesgo, analizando el mismo desde el enfoque de la protección de los derechos y libertades del usuario, disponiendo a su vez de medidas de seguridad de datos personales apropiadas, técnicas u organizativas, para evitar que se realice el supuesto concreto analizado, en este caso, contrataciones online en nombre del titular de los datos

Quedamos a su disposición para cualquier duda o cuestión que pudiera surgir.

Reciba un cordial un saludo,

Área de Protección de Datos de ECIJA
info@ecija.com
Telf: + 34 91.781.61.60