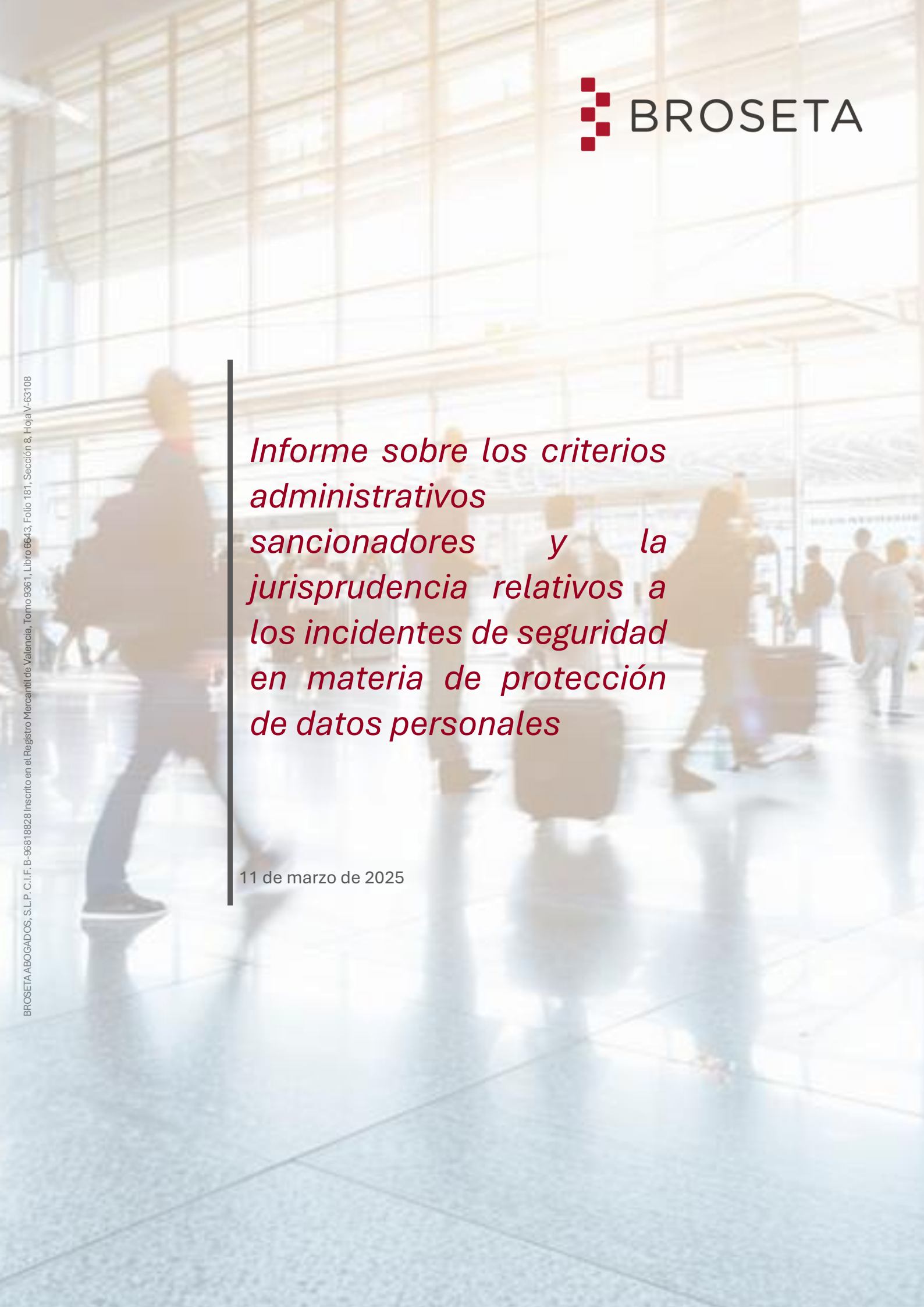

Informe sobre los criterios administrativos sancionadores y la jurisprudencia relativos a los incidentes de seguridad en materia de protección de datos personales

11 de marzo de 2025

I.- INTRODUCCIÓN Y OBJETO

El objeto de este informe es exponer los criterios aplicados por la Agencia Española de Protección de Datos en sus recientes resoluciones de los procedimientos sancionadores incoados como consecuencia de la producción de las denominadas brechas de seguridad ("*data breach*", por sus siglas en inglés) y que han dado lugar a la imposición de multas de importes relevantes a los distintos responsables del tratamiento. En el presente informe, se exponen igualmente determinados criterios de la jurisdicción revisora de las actuaciones de dicha autoridad de control.

La Agencia Española de Protección de Datos (en adelante, indistintamente, "**AEPD"** o la **"Agencia"**) ha iniciado en los últimos años numerosos procedimientos sancionadores relacionados con la existencia de ataques y ciberataques en los sistemas y recursos en los que se tratan datos personales de personas físicas tales como clientes, potenciales clientes, empleados o candidatos de compañías de distintos sectores, que han afectado a la confidencialidad, integridad o disponibilidad (temporal o definitiva) de dichos datos.

De este modo, la AEPD ha venido imponiendo numerosas multas de importe significativo a empresas lo que le ha llevado a posicionarse como la autoridad europea más activa en la aplicación del RGPD en este ámbito desde la plena aplicación del Reglamento (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante, indistintamente, "**RGPD**" o el "**Reglamento**"), declarando la existencia de más de 100 infracciones por la aplicación de los artículos 5.1 f) y/o 32 del RGPD. Solo en 2024 se dictaron 21 resoluciones sancionadoras derivadas de la existencia de brechas de seguridad, por un importe de 12,8 millones de euros (casi el 50% del total de sanciones impuestas), habiendo afectado, en particular, a los sectores del *retail*[1], energía[2], banca[3], seguros[4] y telecomunicaciones[5].

En concreto, y al margen de otras posibles sanciones derivadas de las circunstancias del caso concreto, la AEPD ha considerado que en estos supuestos podían haberse cometido infracciones por (i) la vulneración del principio de confidencialidad e integridad de los datos (art. 5.1.f RGPD); (ii) la ausencia de medidas de seguridad conforme a una adecuada evaluación de riesgos (artículo 32.1 del RGPD); y (iii) la inexistencia de una adecuada protección de datos desde el diseño y por defecto (artículo 25 del GDPR).

---

[1] Resolución del Procedimiento núm. PS/00084/2023 por un importe total de 6.5 millones de euros.

[2] Resoluciones de los Procedimientos núm. PS/00002/2023, PS/00145/2023 y PS/00221/2023 (estas dos últimas a empresas pertenecientes al mismo grupo por una misma brecha de seguridad) por importes totales, respectivamente de 6.5, 3.5 y 3 millones de euros.

[3] Resoluciones de los Procedimientos núm. PS/00020/2023, PS/00331/2022 y PS/00677/2022 por importes totales, respectivamente, de 5, 2. y un millón de euros, así como un total de 26 resoluciones a varias entidades pertenecientes al mismo grupo, adoptadas en enero de 2025, por una única brecha de seguridad por un importe total de en torno a 1,2 millones de euros.

[4] Resolución del Procedimiento núm. PS/00453/2023 por un importe total de 5 millones de euros.

[5] Resoluciones de los Procedimientos núm. PS/00059/2020 y PS/00291/2023 por importes totales, respectivamente, de 3.94 y 1.3 millones de euros.

De forma ejecutiva, la AEPD considera que:

- El artículo 5.1.f del RGPD se infringe cuando se produce una pérdida de confidencialidad o integridad, haya o no ausencia y/o una eventual deficiencia de medidas de seguridad;

- El artículo 32.1 del RGPD se considera infringido cuando ha quedado acreditada la insuficiencia en las medidas, técnicas y organizativas, exigibles para garantizar un nivel de seguridad adecuado a los riesgos generados por el tratamiento; y

- El artículo 25 del GDPR se infringiría en caso de apreciarse por la AEPD que, al margen de las medidas de seguridad mencionadas, no se han adoptado otras medidas técnicas y organizativas adecuadas al riesgo derivado del tratamiento.

Como se ha indicado, juntos con las anteriores infracciones, la AEPD ha considerado en ocasiones infringidas otras obligaciones previstas en el RGPD, tales como la ausencia de notificación de la brecha de seguridad a la autoridad de control (artículo 33) o a los interesados (34), así como la inexistencia de una adecuada evaluación de impacto en la protección de datos (artículo 35). Con carácter general, señalamos que, en los expedientes relacionados con brechas de seguridad se haya apreciado la vulneración de otros principios del tratamiento previstos en el artículo 5.1 del RGPD ni la ilicitud de dicho tratamiento (conforme a los artículos 6.1 y 9 en el caso de datos pertenecientes a categorías especiales).

II.- CONCEPTO Y TIPOS DE BRECHAS DE SEGURIDAD

A los efectos del RGPD, el concepto de brecha de seguridad se identifica con el de "*violación de la seguridad de los datos personales* que se define como "*toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos*".

Esta definición nos permite diferenciar entre tres tipos posibles de brechas de seguridad (si bien una sola brecha puede pertenecer a varias de estas categorías):

- Brechas de confidencialidad, en que los datos personales han podido ser accedidos por terceros sin autorización, incluyendo los supuestos de exfiltración de datos.

- Brechas de disponibilidad, en que los datos han permanecido inaccesibles de forma temporal o permanente para quien legítimamente debe poder tratarlos o acceder a ellos.

- Brechas de integridad, en que se han alterado los datos personales de forma ilegítima pudiendo causar un daño a los afectados.

III.- PROCEDIMIENTO EN CASO DE DETECCIÓN DE UNA BRECHA

1. Procedimiento general.

Cuando se haya detectado la existencia de una brecha de seguridad, y además de las actuaciones que deben llevarse a cabo de forma inmediata para evitar su continuación (adopción de medidas reactivas inmediatas de contención) la normativa de protección de datos personales impone al interesado una serie de obligaciones específicas. Así:

- Deberá procederse de forma inmediata a analizar la severidad de la brecha de seguridad. Existen a tal efecto distintas metodologías, entre las que puede hacerse referencia al recurso "notifica brecha" disponible en la página web de la AEPD o la contenida en el documento "*Recommendations for a methodology of the assessment of severity of personal data breaches*", adoptado por la European Union Agency for Cybersecurity ("**ENISA**").

- En caso de que el riesgo o severidad de la media pueda ser calificado como alto o muy alto deberá igualmente procederse a su notificación a la AEPD. El plazo de dicha notificación es sumamente breve, dado que debe llevarse a cabo en el plazo de 72 horas desde que se tiene conocimiento de la brecha. No obstante, esa notificación puede efectuarse con carácter previsional, completándose con otra posterior, para la que la AEPD otorga un plazo de 30 días hábiles.

- En caso de que la brecha implique un alto riesgo para los derechos y libertades de los interesados deberá procederse igualmente a notificar la misma a aquéllos, incluyendo en dicha notificación no sólo una descripción de lo sucedido, sino de las medidas adoptadas y de las que los interesados puedan adoptar para minimizar los efectos de la brecha de seguridad.

Es importante indicar que estas obligaciones corresponden al responsable del tratamiento. Por este motivo, si la brecha se produce en los sistemas del encargado del tratamiento será preciso que el mismo informe inmediatamente acerca de su existencia al responsable, que habrá de notificarla a la AEPD. Los contratos de encargo del tratamiento suelen establecer para ello plazos breves que nunca deberían exceder de las 48 horas. Destacamos que la AEPD ha reconocido la posibilidad de que el encargado realice la notificación, aunque deberá contar con una autorización fehaciente del responsable en este sentido (por ejemplo, a través de correo electrónico)[6].

La notificación de la brecha a la AEPD dará lugar a su análisis por su División de Innovación Tecnológica (DIT), que la analizará y clasificará, proponiendo, en su caso, a la Presidencia de la AEPD la iniciación de una investigación.

En este sentido, identificación y notificación (en forma y plazo) de una brecha de seguridad no implica (no debería implicar) automáticamente la apertura de una investigación[7]. No obstante, la misma podrá tener lugar en dos casos:

[6] Resolución de los Procedimientos núm. PS/00003/2024 a PS/00027/2024, disponibles en www.aepd.es/informes-y-resoluciones/resoluciones.

[7] Notificación de Brechas de Datos personales a la Autoridad de Control (AEPD), accesible en: https://www.aepd.es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/brechas-de-datos-personales-notificacion.

- Cuando así lo decida la Presidencia de la AEPD, a propuesta de la precitada División de Innovación Tecnológica.
- Cuando se dirijan reclamaciones por los interesados cuyos datos han quedado comprometidos ante la AEPD. En este caso, la AEPD puede solicitar al Delegado de Protección de Datos del notificante información adicional y, en su caso, admitir a trámite la brecha, lo que daría lugar al inicio de la investigación.

En caso de iniciarse la investigación, la AEPD podrá requerir a los involucrados (responsable o encargado del tratamiento) por la brecha la información que resulte necesaria para un mejor conocimiento de los hechos. Estas actuaciones tendrán una duración máxima de 18 meses y concluirán mediante decisión que acuerde (i) el archivo del expediente; o (ii) la apertura de un procedimiento sancionador, que se tramitará durante un plazo máximo de 12 meses adicionales.

2.- Especialidades en relación con las brechas relacionadas con tratamientos transfronterizos de datos.

En el seno de los grupos multinacionales puede plantearse el problema de que una misma brecha afecte a distintas entidades del Grupo ubicadas en distintos Estados miembros del Espacio Económico Europeo (e.g. una brecha que afecta a un fichero centralizado de clientes de diversas empresas del Grupo) o que la brecha afecte a un único tratamiento que se refiera a interesados que se encuentren en más de un Estado Miembro. En ese último caso, debe tenerse en cuenta que el RGPD establece reglas específicas para la tramitación del procedimiento, aplicando el mecanismo de ventanilla única (*one-stop shop*), en cuya virtud una empresa con filiales en varias jurisdicciones deberá relacionarse únicamente con la denominada autoridad de control principal.

Por lo tanto, una vez producida la brecha la primera cuestión será determinar si el tratamiento afectado tiene o no carácter transfronterizo[8] y, en este caso, determinar qué autoridad de protección de datos deberá ser considerada autoridad de control correspondiente al establecimiento principal[9].

Si el tratamiento es transfronterizo, esta autoridad será la competente para la tramitación del procedimiento, que se someterá a las normas del procedimiento coordinado establecido en el RGPD. Ello implica que las notificaciones se llevarán a cabo ante dicha autoridad, que dará cuenta de la evolución del procedimiento a las autoridades de los restantes Estados Miembros afectados por la brecha de seguridad, pudiendo éstas participar en el procedimiento a través de

[8] Definido como "*a) el tratamiento de datos personales realizado en el contexto de las actividades de establecimientos en más de un Estado miembro de un responsable o un encargado del tratamiento en la Unión, si el responsable o el encargado está establecido en más de un Estado miembro, o b) el tratamiento de datos personales realizado en el contexto de las actividades de un único establecimiento de un responsable o un encargado del tratamiento en la Unión, pero que afecta sustancialmente o es probable que afecte sustancialmente a interesados en más de un Estado miembro*" (art 4.23 del RGPD).

[9] Es decir, la correspondiente al establecimiento "*en lo que se refiere a un responsable del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión, salvo que las decisiones sobre los fines y los medios del tratamiento se tomen en otro establecimiento del responsable en la Unión y este último establecimiento tenga el poder de hacer aplicar tales decisiones, en cuyo caso el establecimiento que haya adoptado tales decisiones se considerará establecimiento principal*" (artículo 4.16 a) del RGPD).

la emisión de las denominadas objeciones pertinentes motivadas. Igualmente, si no existe un acuerdo en lo que respecta a la decisión final del procedimiento, el Comité Europeo de Protección de Datos emitirá un dictamen vinculante, al que se someterá la decisión final adoptada.

Es importante indicar que en el supuesto de que una empresa lleve a cabo múltiples actividades de tratamiento transfronterizo y las decisiones relativas a los fines y los medios del tratamiento se adopten en distintos establecimientos (e.g. porque, en el caso de tratamientos relacionados con Recursos Humanos, los datos tratados por cada entidad difieren conforme a las exigencias de su derecho laboral nacional), no será de aplicación el procedimiento coordinado, de forma que cada autoridad será competente para la tramitación del procedimiento respecto de la filial correspondiente.

Finalmente, el mecanismo de cooperación y coherencia del RGPD se aplica únicamente en caso de que los responsables cuenten con uno o más establecimientos en el Espacio Económico Europeo. En caso de que una empresa no disponga de un establecimiento en el mismo, la responsable deberá interactuar con cada una de las autoridades de control locales de cada Estado miembro.

IV.- SUJETOS RESPONSABLES

Entrando ya en el análisis de las resoluciones de la AEPD y las sentencias existentes en la materia, la primera cuestión que debe analizarse es la de determinar el sujeto que sería responsable de la infracción que en su caso se apreciase como consecuencia de la existencia de una brecha de seguridad.

En este sentido, debe recordarse que, junto con la figura del responsable del tratamiento, que decide sobre los medios y fines del mismo, las normas de protección de datos regulan la figura del encargado del tratamiento, al que el responsable encomienda la prestación de un servicio que implica el tratamiento de datos personales y que el encargado únicamente llevará a cabo siguiendo sus instrucciones, sin decidir en ningún caso sobre los fines y medios de dicho tratamiento.

De este modo, el encargado no posee ningún interés propio respecto del resultado del tratamiento objeto del encargo, actuando en nombre y por cuenta del responsable.

La Sentencia del Tribunal de Justicia de la Unión Europea de 5 de diciembre de 2023, (asunto C-683/21), se refiere a la posibilidad de que el responsable sea sancionado por las operaciones de tratamiento desarrolladas por un encargado del tratamiento, indicando que dicho responsable no solo responde por el tratamiento de datos personales que lleve a cabo directamente, sino también por aquellos tratamientos realizados en su nombre. Este principio sólo se vería alterado en caso de que fuera aplicable el artículo 28.10 del RGPD, por destinar el encargado los datos a sus propios fines, excediendo los límites del encargo.

Se establece así un modelo de responsabilidad del responsable del tratamiento no solo por estar obligado a seleccionar un encargado que acredite el cumplimiento de la norma (culpa *in eligendo*), sino también como consecuencia de su deber de supervisión constante de su

actuación (culpa *in vigilando*), garantizando en todo momento que el tratamiento de los datos por el encargado se realice con estricto cumplimiento de la normativa aplicable.

Esta doctrina se ha plasmado por la AEPD a sus resoluciones sancionadoras en relación con las brechas de seguridad, que ha considerado, con carácter general, que se dirigirán contra el responsable por la posible infracción del RGPD en la actuación de sus encargados del tratamiento[10], salvo en aquellos casos en los que estos últimos hayan actuado como verdaderos responsables del tratamiento, decidiendo sobre los fines y medios del tratamiento[11].

En este sentido, no sólo hay que tener en cuenta que el RGPD impone al responsable las obligaciones derivadas con la notificación de las brechas de seguridad, así como las relacionadas con la realización del análisis de riesgos y la adopción de las correspondientes medidas técnicas y organizativas que mitiguen el riesgo que el tratamiento puede tener en los derechos y libertades de los interesados, sino que, igualmente, el artículo 28.3.c del RGPD impone al encargado del tratamiento el deber de adoptar las medidas de seguridad pertinentes en función del riesgo inherente a los tratamientos que lleva a cabo, asegurando que dichas medidas queden debidamente reflejadas en el contrato de encargo suscrito con el responsable del tratamiento, y siendo por ello preciso que el responsable controle su cumplimiento.

En todo caso, la regla mencionada también ha sido objeto de alguna excepción, en la que la AEPD ha imputado exclusivamente la responsabilidad a un encargado del tratamiento[12]. No obstante, se trata de un supuesto excepcional en que han de tenerse en cuenta las especiales circunstancias del caso.

En todo caso, lo indicado anteriormente debe entenderse al margen de la posible acción de repetición que el responsable podría tener contra el encargado si se ha acreditado que la brecha se produjo en los sistemas de este último, estándose a las cláusulas de responsabilidad que se hubieran pactado.

V.- PRINCIPALES INFRACCIONES APRECIADAS POR LA AEPD

Como se indicó en el apartado I anterior, la AEPD ha apreciado en sus resoluciones sobre los casos de brechas de seguridad, la afección de los artículos 5.1 f), 32 y 25 del RGPD. Nos referimos a continuación a la interpretación dada por la AEPD a dichas normas.

1.- Vulneración del principio de confidencialidad e integridad

Conforme establece el artículo 5.1 f) del RGPD, los datos serán "*tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el*

[10] *Op. cit.* Procedimientos núm. PS/00003/2024 a PS/00027/2024.

[11] La Sentencia de la Audiencia Nacional, Sala de lo Contencioso-Administrativo, Sección 1ª, núm. 595/2024, de 8 de febrero de 2024, establece que "*no ha quedado acreditado que las citadas empresas, como encargadas del tratamiento de la parte actora, hayan determinado fines y medios del tratamiento, ni hayan utilizado los datos de los clientes de aquella para sus propias finalidades, ni han interactuado frente a los interesados ajenos a la estructura y nombre comercial de la sociedad recurrente, sino que han actuado bajo el nombre de la parte actora para el cumplimiento de los fines de estos, utilizando los sistemas de ésta para realizar las operaciones con los clientes. Por lo que, no cabe invocar el art. 28.10 del RGPD para una presunta atribución de responsabilidad a los encargados que, además, implique la exoneración del responsable del tratamiento, es decir, de la sociedad aquí recurrente*".

[12] Resolución del Procedimiento núm. PS/00145/2023, accesible en: www.aepd.es/documento/ps-00145-2023.pdf.

tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas".

En consecuencia, los datos personales deben ser tratados de forma que se garantice su confidencialidad, integridad y disponibilidad, mediante la aplicación de medidas técnicas y organizativas apropiadas. Es importante tener en cuenta que la AEPD reitera[13] que estas medidas no se limitan estrictamente a las que garantizan la seguridad de los datos, sino que pueden referirse a medidas de toda índole (por ejemplo, disponer de un procedimiento sólido de atención a reclamaciones[14], garantizar una configuración de los tratamientos que garantice el principio de minimización en los accesos a los datos[15], etc.).

En este sentido, los responsables del tratamiento tienen la obligación de evaluar los riesgos asociados al tratamiento de datos personales, teniendo en cuenta su probabilidad y gravedad en relación con los derechos y libertades de las personas físicas. Este análisis deberá ser exhaustivo, tomando en cuenta estos riesgos potenciales a partir de su posible concurrencia[16], aun cuando la misma no se daría en condiciones normales. A partir de esta evaluación y análisis, deberán implementar medidas técnicas y organizativas apropiadas que aseguren la aplicación efectiva de los principios de protección de datos. Este enfoque, basado en el análisis de riesgos, constituye un pilar fundamental del RGPD[17].

Conforme a las resoluciones de la AEPD, el contenido del artículo 5.1.f) establece, en definitiva, una obligación de resultado, dado que las resoluciones han ido evolucionando hacia un razonamiento en que se imputa la comisión de esta infracción por el hecho de haberse producido la mera pérdida de confidencialidad, integridad o disponibilidad de los datos personales[18].

En este sentido, la AEPD argumenta esta obligación de resultado por cuanto, si bien reconoce la posibilidad de que se produzca un incidente de seguridad - pues ningún sistema o recurso implementado para evitarlo es invulnerable- exige que dicho escenario debe estar contemplado y evaluado como parte del análisis de riesgos, a fin de (i) implementar las medidas técnicas y organizativas adecuadas para prevenirlo; y (ii) establecer las acciones necesarias para minimizar los daños en caso de que llegue a materializarse. Así, concluye la autoridad de control que si se produce una brecha de seguridad, ello implica que las acciones han fallado y la conducta es sancionable[19].

---

[13] Resoluciones de los Procedimientos núm. PS/00677/2022, PS/00145/2023 y PS/00291/2023.
[14] *Op. cit.* Procedimiento núm. PS/00145/2023.
[15] Resolución del Procedimiento núm. PS/00453/2023, accesible en: www.aepd.es/documento/ps-00453-2023.pdf.
[16] La Resolución de la AEPD recaída en el procedimiento PS/00677/2022, establece que "l*a pérdida accidental, el olvido o el robo de las claves o credenciales de un cliente es algo más que habitual. Que otra persona pueda, de manera fortuita o no, tener acceso a las claves o credenciales de otra distinta tampoco es nada extraño.* […] *Que una persona pueda acceder a la banca digital de un cliente por la causa descrita no es imprevisible.* […] *Simplemente es algo que sucede. Nos encontramos de esta forma con un riesgo palpable presente en el tratamiento, que aun en este momento la entidad bancaria sigue sin identificar, sin evaluar y sobre el que no ha establecido ni se previeron medidas técnicas u organizativas de ningún tipo*". Accesible en: www.aepd.es/documento/ps-00677-2022.pdf.
[17] Resolución del Procedimiento núm. PS/00020/2023, accesible en: www.aepd.es/documento/ps-00020-2023.pdf.
[18] Resoluciones de los Procedimientos núm. PS/00145/2023, PS/00291/2023 y PS/00453/2023.
[19] *Op. cit.* Procedimiento núm. PS/00020/2023.

De este modo, si la brecha es de confidencialidad, la AEPD afirma que cualquier exposición o tratamiento no autorizado de datos personales constituye una infracción del principio de confidencialidad, tal como establece el artículo 5.1.f del RGPD, dado que ha tenido que existir un fallo en las medidas que debían adoptarse para evitarla.

Por otra parte, respecto de las brechas de disponibilidad, la AEPD aprecia que esta circunstancia se dará no sólo cuando los datos no estén disponibles para el responsable, sino también en los casos en los que los datos no se encontraron, temporal o definitivamente, a disposición del interesado a través de los canales puestos a su disposición por el responsable del tratamiento[20].

Es asimismo relevante destacar que no es necesario que se produzca un daño tangible para que se considere cometida la infracción. En este sentido, el considerando 85 del RGPD establece que la pérdida de confidencialidad e integridad puede suponer un riesgo que conlleve daños físicos, materiales o inmateriales, evidenciando que no es imprescindible un perjuicio económico o tangible para considerar vulnerado el derecho del interesado, siendo a juicio de la AEPD este riesgo, el daño causado al interesado[21].

2.- Ausencia de medidas de seguridad adecuadas

El artículo 32 del RGPD establece la obligación de adoptar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, centrándose únicamente en la seguridad del tratamiento. Estas medidas deben establecerse considerando el estado de la técnica, los costes de aplicación, así como la naturaleza, el alcance, el contexto y las finalidades del tratamiento, además de los riesgos, cuya probabilidad y gravedad puede variar, para los derechos y libertades de las personas físicas.

Respecto de esta obligación, la STS de 15 de febrero de 2022 considera que no es de resultado, sino de medios. La AEPD considera en este sentido que debe evaluarse la diligencia de los responsables y encargados en la implementación de dichas medidas previa evaluación de los riesgos derivados del tratamiento para los derechos y libertades de los interesados.

La evaluación del riesgo debe ser dinámica. De este modo, la obligación impuesta por el artículo 32 del RGPD no sólo debe llevarse a cabo en el momento inicial del tratamiento, sino revisarse y actualizarse de forma permanente, a través de un modelo de gestión continua del riesgo y de adaptación progresiva a los nuevos riesgos que puedan surgir a lo largo del tiempo.

Además, no será suficiente que se hayan evaluado los riesgos y documentado las medidas destinadas a su mitigación, sino que será necesario que dichas medidas se hayan implementado real y eficazmente y se cuente con un proceso de revisión continua que permita verificar tanto su implementación como su eficacia[22].

[20] *Op. cit.* Procedimiento núm. PS/00020/2023.
[21] *Op. cit.* Procedimiento núm. PS/00453/2023.
[22] La Resolución del Procedimiento núm. PS/00677/2022, establece, por ejemplo, que "*la existencia de negligencia en el cumplimiento y observancia de las medidas adecuadas para garantizar la seguridad necesaria para la protección de los datos personales, concretamente para garantizar la confidencialidad de los datos personales, por cuanto no adoptó medidas dirigidas a ello, en especial las que indicó en las EIPD para mitigar los riesgos "altos" y "muy altos" consistentes en adoptar medidas de cifrado, pseudonimización o anonimización*".

Por otra parte, la AEPD considera que la evaluación previa a la adopción de las medidas de seguridad debe focalizarse en los riesgos que puedan afectar a los derechos y libertades de las personas titulares de los datos personales y no en los riesgos de seguridad que impacten únicamente a la organización, considerando insuficiente la adopción de medidas basadas en la preservación de la disponibilidad, integridad y confidencialidad de la información de la organización. Ello conduce a la conclusión de que, si bien la adopción de estándares (e.g. ISO 27001 u otras certificaciones) puede tomarse como referencia y facilita el cumplimiento, ello no implica automáticamente el cumplimiento del artículo 32 del RGPD, al diferenciarse el análisis de seguridad en el seno de la organización del resultante de la evaluación de riesgos mencionada[23].

3.- Posible concurrencia de las infracciones de los artículos 5.1 f) y 32 del RGPD

En un gran número de resoluciones la AEPD analiza la compatibilidad de la imposición de las sanciones previstas en los artículos 5.1 f) y 32 del RGPD, dado que las entidades contra las que se dirigen los procedimientos alegan en defensa de su derecho la concurrencia del principio *non bis in idem* o la existencia de un concurso medial, dado que la infracción del artículo 32 sería el que ha conducido, a su vez, a la del principio de confidencialidad e integridad de los datos.

La postura de la AEPD hasta ese momento, y desde que la sentencia de 15 de febrero de 2022 considerase la obligación de adopción de medidas de seguridad como una obligación de medios y no de resultado, ha sido la de apreciar la inexistencia de *bis in idem* o concurso medial sobre la base de que la brecha de seguridad no sólo se ha debido a la insuficiencia de las medidas adoptadas. Así, se ha indicado que, pueden darse situaciones en las que las medidas técnicas y organizativas sean inadecuadas, pero no se produzca una pérdida efectiva de los datos, así como escenarios en los que, aun siendo las medidas de seguridad técnicamente adecuadas, éstas no evitan la pérdida de confidencialidad, integridad o disponibilidad[24]. No obstante, en la práctica, la actuación supone la apreciación de una infracción tanto en los medios (las medidas de seguridad) como en el resultado (la brecha de seguridad), habiendo sido habitual la imposición de ambas sanciones.

Sin embargo, es relevante tener en cuenta que la sentencia del Audiencia Nacional de 8 de febrero de 2024, referida a un supuesto en que la AEPD únicamente sancionaba la vulneración del artículo 5.1 f) del RGPD, indica que el ámbito de este artículo y el artículo 32 del RGPD no son idénticos, dado que la obligación de adoptar medidas de seguridad no circunscribe el principio de confidencialidad e integridad en su totalidad. Esta afirmación puede igualmente interpretarse en el sentido de que aun cuando la integridad del principio de confidencialidad sea más amplia que la obligación de adoptar medidas de seguridad, esta obligación sí quedaría incluida en el artículo 5.1 f) del RGPD si la confidencialidad se ha visto únicamente

[23] Resoluciones de los Procedimientos núm. PS/00003/2024 a PS/00027/2024 y PS/00084/2023.

[24] La Resolución del Procedimiento núm. PS/00677/2022, establece que la parte reclamada "*había implementado medidas adecuadas desde el punto de vista de la seguridad para impedir el riesgo, aun cuando, desafortunadamente, dichas medidas fallaron en el presente caso*".

comprometida como consecuencia de una insuficiencia de las medidas de seguridad adoptadas. En el mismo sentido se pronuncia el TS en su sentencia de 8 de octubre de 2024.

Esta doctrina se ha plasmado en recientes resoluciones de la AEPD, en que se ha apreciado que no procede la sanción por vulneración del artículo 32 del RGPD si no se ha detectado la insuficiencia de ninguna medida de seguridad distinta de las que han dado lugar a la pérdida de confidencialidad de los datos[25].

4.- Protección de datos desde el diseño y por defecto

En virtud del artículo 25 del RGPD, el responsable o encargado del tratamiento está obligado a aplicar, tanto al determinar los medios del tratamiento como durante el propio tratamiento, medidas técnicas y organizativas apropiadas, diseñadas para garantizar la aplicación efectiva de los principios de protección de datos. La AEPD considera que esta obligación, a diferencia de la establecida en el artículo 32, no se limita únicamente a medidas de seguridad, sino a medidas de toda índole, siendo su finalidad asegurar que la protección de datos personales se integre plenamente en la estructura y el funcionamiento ordinario de la organización, convirtiéndose en un elemento esencial desde el inicio del tratamiento de datos personales[26].

En este contexto, la AEPD recuerda la protección de datos debe ser considerada tanto en las etapas iniciales como durante la toma de decisiones o la planificación de los procesos. Esta obligación requiere un enfoque continuo de revisión y mejora. La organización debe llevar a cabo evaluaciones periódicas para determinar si las medidas técnicas y organizativas implementadas son adecuadas para garantizar el cumplimiento del RGPD y salvaguardar los derechos de los interesados, promoviendo un sistema dinámico de retroalimentación y actualización constante.

En particular, la AEPD indica, de nuevo, que el enfoque no debe estar orientado hacia los riesgos que puedan afectar a la organización, sino hacia aquellos que puedan afectar a los derechos y libertades de protección de datos personales de los interesados, rechazando las medidas que se adoptan sobre la base de la evaluación de riesgos legales o tecnológicos para la empresa, por entender dichos análisis insuficientes a los efectos del RGPD[27]. Así, la AEPD se ha referido en ocasiones a que los documentos aportados por las entidades investigadas para acreditar la seguridad de sus sistemas no se refieren expresamente a términos como "*datos personales*" o "*protección de datos de carácter personal*"[28].

Tampoco se considera adecuado el análisis desarrollado si la documentación asociada fue elaborada antes de la plena aplicación del RGPD; si no se identifican ni evalúan todos los posibles

[25] Las Resoluciones de los procedimientos núm. PS/00003/2024 a PS/00027/2024, establecen que "*revisadas las alegaciones formuladas por la parte reclamada, y en atención a las mismas, revisada la documentación obrante en el expediente administrativo y la aportada por la parte reclamada, se evidencia que todas las medidas técnicas y organizativas de seguridad cuya ausencia ha quedado probada, posibilitando directamente la brecha de datos personales, sin que se haya producido una conculcación, en el caso concreto, del artículo 32 del RGPD a no haberse acreditado la ausencia de otras medidas técnicas y organizativas de seguridad independientes de la brecha de datos personales*".

[26] Resoluciones de los Procedimientos núm. PS/00677/2022 y PS/00020/2023

[27] Resoluciones de los Procedimientos núm. PS/00677/2022, PS/00020/2023, PS/00084/2023 y PS/00453/2023

[28] *Op. cit.* Procedimiento núm. PS/00020/2023

riesgos que pueden afectar a los derechos y libertades de los interesados, o si el enfoque adoptado otorga prioridad a los riesgos organizacionales por encima de los riesgos que afectan a los interesados (incluso en los supuestos en que ambos inciden necesariamente el uno en el otro[29]).

Por otro lado, también merece el reproche de la AEPD si el responsable adopta una actitud meramente reactiva, limitándose a atender exclusivamente las cuestiones que le son requeridas, sin actuar de manera sistemática, preventiva y global, pues a juicio de dicha autoridad de control, ello evidencia la falta de una estrategia orientada a la protección de datos desde el diseño y por defecto y la consiguiente infracción de este artículo[30].

5.- Notificación de una violación de la seguridad

De acuerdo con el artículo 33 del RGPD, el responsable del tratamiento está obligado a notificar a la autoridad de control competente cualquier violación de la seguridad de los datos personales a más tardar en un plazo de 72 horas desde el momento en que tenga constancia de la misma. Se exceptúan aquellos supuestos en los que sea improbable que la brecha suponga un riesgo para los derechos y libertades de las personas físicas.

El Reglamento no especifica un umbral concreto de probabilidad ni exige que el riesgo se haya materializado para que la notificación sea obligatoria; basta con que exista la posibilidad de que dicho riesgo ocurra. En este sentido, la simple pérdida de confidencialidad de los datos personales constituye un riesgo probable, lo que hace necesaria la notificación a la autoridad de control[31].

Cuando la notificación se realiza fuera del plazo establecido, sin justificación válida que acredite la demora, se vulnera la obligación de comunicación oportuna establecida en el RGPD. En estos casos, la falta de diligencia en la gestión del incidente de seguridad puede constituir una infracción sancionable, especialmente si el responsable del tratamiento tuvo conocimiento del hecho y demoró su notificación más allá del tiempo previsto en la normativa[32].

Asimismo, el artículo 34 del RGPD establece la obligación de comunicar la brecha de seguridad a los interesados cuando el incidente suponga un alto riesgo para sus derechos y libertades. No es necesario que el daño se haya materializado para que esta obligación sea exigible, ya que el riesgo de que los afectados sean víctimas, por ejemplo, de suplantación de identidad, fraude, *phishing* u otros ciberataques, es suficiente para justificar la notificación.

Para que esta comunicación sea efectiva, debe explicarse de manera clara y precisa la naturaleza de la violación y sus posibles consecuencias, detallar las acciones emprendidas por el responsable del tratamiento para contener el incidente e incluir recomendaciones concretas para que los afectados puedan proteger sus datos y minimizar el riesgo.

---

[29] La Resolución del Procedimiento núm PS/00677/2022, establece, por ejemplo, que los riesgos derivados de suplantación de identidad en las entidades de crédito, que suponen tanto un perjuicio para ésta como para el interesado suplantado, son también considerados riesgos de la organización.
[30] *Op. cit.* Procedimientos núm. PS/00020/2023 y PS/00453/2023.
[31] Resolución del Procedimiento núm. PS/00002/2023, accesible en: www.aepd.es/documento/ps-00002-2023.pdf.
[32] Resolución del Procedimiento núm. PS/00179/2020, accesible en: www.aepd.es/documento/ps-00179-2020.pdf.

En este sentido, una comunicación deficiente que no informe adecuadamente a los interesados sobre el alcance y las implicaciones de la violación podría impedir que estos adopten las medidas oportunas y, en consecuencia, incrementar su vulnerabilidad frente a potenciales ataques o fraudes. No basta con una simple notificación formal, sino que es imprescindible que el mensaje sea accesible, comprensible y contenga instrucciones claras sobre cómo proceder en caso de que los datos personales hayan sido comprometidos[33].

VI.- CUESTIONES RELACIONADAS CON LA CULPABILIDAD Y LA RESPONSABILIDAD

1.- Exigencia de dolo o negligencia en la actuación del responsable. La diligencia debida del responsable.

Como se ha venido indicando, la jurisprudencia del Tribunal Supremo (STS de 15 de febrero de 2022) indica que la obligación de adopción de medidas de seguridad constituye una obligación de medios y no de resultado. En esta misma línea, el artículo 25 del RGPD impone una obligación de medios, consistentes en la implementación de medidas técnicas y organizativas adecuadas para asegurar la aplicación efectiva de los principios de protección de datos desde el diseño y por defecto.

De este modo, la mera existencia de una brecha de seguridad no determina por sí sola la apreciación de una infracción de estos preceptos, sino que es necesaria la ausencia de medidas razonables y adecuadas al nivel de riesgo generado por cada tratamiento.

La cuestión entonces se plantea en referencia a la aplicación del artículo 5.1.f del RGPD, dado que la ruptura de la confidencialidad, disponibilidad o integridad de los datos (es decir, el resultado) podría determinar la comisión de la infracción de dicha norma.

No obstante, conforme a los principios del derecho sancionador (similares a los del derecho penal) para que pueda apreciarse la responsabilidad en este caso no puede ser suficiente la mera materialización del resultado, sino que será preciso analizar las circunstancias del caso y determinar si la infracción se originó como consecuencia de una actuación negligente o dolosa del responsable, no siendo aplicable una responsabilidad objetiva por la mera producción del resultado (la brecha de seguridad). En este sentido, la sentencia de la Audiencia Nacional de 17 de octubre de 2007 establece que el principio de culpabilidad impide la imposición de sanciones basadas en la responsabilidad objetiva dentro del ámbito del Derecho administrativo sancionador.

Así lo pone de manifiesto la AEPD en sus resoluciones, negando expresamente que quepa respecto de ninguna de las tres infracciones relacionadas con los incidentes de seguridad la aplicación del principio de responsabilidad objetiva, indicando que la imputación al responsable se funda en un análisis individualizado de las circunstancias y de la concurrencia de culpabilidad del responsable, de forma que concurra ésta a título de dolo o de culpa.

[33] *Op. cit.* Procedimiento núm. PS/00002/2023.

Ahora bien, en el caso de infracciones cometidas por personas jurídicas, el elemento culpabilístico se traduce, siguiendo la STS de 23 de enero de 1998, en la ausencia de la diligencia que resultaba exigible a la entidad contra la que se dirige el procedimiento. Es decir, no basta, para la exculpación frente a un comportamiento típicamente antijurídico, la invocación de la ausencia de culpa, sino que es precisa la acreditación de que se ha obrado con la diligencia exigible.

En este contexto, considera la AEPD que cuando una persona jurídica no implementa las medidas técnicas y organizativas adecuadas, no acreditando en consecuencia haber actuado con la diligencia debida en función del nivel de riesgo y las concretas circunstancias del tratamiento, queda acreditada la existencia de un comportamiento negligente, suficiente para apreciar la culpabilidad.

A partir de esta premisa, el carácter doloso o negligente de la infracción se evaluará teniendo en cuenta los elementos objetivos de conducta derivados de los hechos del asunto, valorando la naturaleza, el alcance, el contexto y los fines de cada tratamiento, y determinando el grado de culpabilidad caso por caso.

En este punto es especialmente relevante, en materia de brechas de seguridad, tener en cuenta que, como indica la Sentencia de la Audiencia Nacional de 22 de junio de 2021, la culpabilidad del infractor no puede considerarse excluida por el hecho de que se haya producido la intervención fraudulenta de un tercero (esto es, el ciber atacante).

En este sentido, la AEPD indica en sus resoluciones, ante la alegación de que la brecha se debe a la intervención de un tercero, que cuando se ha producido un ataque, la implementación de medidas de seguridad adecuadas y eficaces podría haber prevenido el incidente de seguridad o, en su defecto, haber limitado su impacto a un número significativamente menor de interesados o de datos afectados[34].

2.- Aplicación del principio de proporcionalidad. Circunstancias atenuantes y agravantes.

El RGPD establece que cada autoridad de control debe garantizar que la imposición de sanciones administrativas sea efectiva, proporcionada y disuasoria en cada caso concreto, quedando asimismo ajustada al tamaño de la empresa, calculado por su volumen de negocios, lo cual es interpretado conforme a las normas europeas de derecho de la competencia, es decir, atendiendo al volumen de negocio del grupo y no al de la concreta entidad afectada por la brecha[35].

Los artículos 83.2 del RGPD y 76.2 de la LOPDGSS establecen una enumeración de las posibles circunstancias a tomar en consideración en la determinación del alcance de la responsabilidad de la entidad contra la que se dirige el procedimiento sancionador y, en consecuencia, en importe de la sanción económica a imponer en su caso.

[34] Resoluciones de los Procedimientos núm. PS/00677/2022, PS/00002/2023, PS/00084/2023, PS/00145/2023, PS/00221/2023 y PS/00677/2022.
[35] Resolución del Procedimiento núm. PS/00331/2022, accesible en: www.aepd.es/documento/ps-00331-2022.pdf.

Es relevante tener en cuenta que el régimen sancionador del RGPD establece únicamente los límites máximos de las sanciones económicas que podrían llegar a imponerse, sin establecer ninguna modulación al respecto. Al propio tiempo, la catalogación de las infracciones en leves, graves o muy graves, efectuada por los artículos 72 a 74 de la LOPDGDD lo es únicamente a efectos de su prescripción (no establecida en el RGPD), por lo que puede darse el caso de que una infracción catalogada como grave pueda ser objeto de una sanción superior a la de otra que se catalogue como muy grave por la LOPDGDD.

En este contexto, destacamos que el Comité Europeo de Protección de Datos adoptó las Directrices 04/2022, sobre el cálculo de las multas administrativas contempladas en el RGPD, de remisión constante en las resoluciones de la AEPD, si bien, a nuestro parecer, las mismas no implican la aplicación de criterios completamente terminantes en esta materia.

Hechas estas consideraciones, se hace referencia a continuación a las circunstancias que habitualmente son tomadas en consideración (o excluidas de la misma) en las resoluciones de la AEPD relacionadas con la comisión de infracciones como consecuencia de una brecha de seguridad:

a) **La referencia genérica a la naturaleza, gravedad y duración de la infracción**, es tomada generalmente en consideración por la AEPD como circunstancia agravante de la responsabilidad, atendiendo a factores como la naturaleza, el alcance o la finalidad del tratamiento en cuestión, el número de interesados afectados y el nivel de perjuicio sufrido por estos.

Así, la AEPD considera concurrente esta circunstancia cuando aprecia la ausencia de un diseño adecuado en los tratamientos de datos personales, especialmente cuando estos afectan operaciones de gran trascendencia para los interesados, como la contratación de productos financieros, de seguros o del sector de la energía, dado que considera que estos tratamientos pueden implicar riesgos de considerable gravedad, tales como el fraude o la suplantación de identidad, lo que no solo compromete la disposición o poder de control de los datos personales por parte del interesado, sino que también puede derivar en eventuales perjuicios de índole patrimonial.

En este punto, se toma particular atención al carácter “sensible” de los datos comprometidos en los incidentes de seguridad, indicando que estos no se limitan exclusivamente a los datos pertenecientes a categorías especiales según el RGPD, sino a otros cuya divulgación puede causar un daño o una angustia inmediata al interesado. Entre estos se incluyen, por ejemplo, los datos de localización; las comunicaciones privadas; los números de identificación nacional o los datos financieros (tales como los extractos de transacciones); los números de tarjetas de crédito o simplemente el número IBAN de la cuenta corriente.

Así por ejemplo, la AEPD ha apreciado que los datos personales vinculados a la contratación de productos financieros o simplemente un número de teléfono pueden dar lugar a diversos riesgos, entre los cuales destacan el fraude, la suplantación de identidad y el uso de técnicas como el *phishing* o la ingeniería social para obtener información adicional de carácter identificativo, cuya pérdida agrava el reproche sancionador.

Igualmente, dentro de esta circunstancia agravante, la AEPD atiende al número de afectados por la brecha y, desde luego, a la cantidad de datos relativos a cada interesado, teniendo en cuenta que cuanto mayor es la misma, mayores son los riesgos para su privacidad.

b) Igualmente, las resoluciones de la AEPD se refieren en la práctica totalidad de los casos a la **intencionalidad o negligencia del responsable** como circunstancia que agrava el reproche sancionador.

En estos casos, frente a la alegación de que el dolo o la culpa son elementos que deben concurrir en todo caso para apreciar la responsabilidad, las resoluciones de la AEPD consideran con carácter general que en estos casos concurre al menos un elevado nivel de negligencia en la conducta del sujeto infractor, en atención a las circunstancias específicas del caso. De este modo, la AEPD considera que, una vez determinado que concurre, como premisa, el elemento subjetivo de culpabilidad, ello no excluye la posibilidad de aplicar la agravante de intencionalidad o negligencia.

La AEPD aprecia esta agravante, de forma reforzada en los supuestos en que el responsable, por su tamaño, experiencia y volumen de datos gestionados, tiene la obligación de actuar con mayor diligencia para garantizar la confidencialidad de los datos personales, considerando que el manejo de una amplia base de datos personales implica mayores riesgos y exige medidas de protección más rigurosas. Además, a grandes organizaciones, con recursos y capacidades técnicas avanzadas, se les exige un estándar más elevado que a pequeñas empresas o individuos[36]. De este modo, esta circunstancia se aplica de forma cuasiautomática en caso de tratarse de empresas con gran volumen de actividad.

c) La AEPD también aprecia como agravante la **vinculación del infractor con la realización de tratamientos de datos personales** que supone una profesionalización de su actividad que impone una mayor diligencia. En este sentido, esta circunstancia ha sido aplicada de forma progresivamente más amplia, refiriéndose en la práctica al mero hecho de que la entidad "está habituada" al tratamiento de datos personales. De esta forma, la AEPD no aprecia la vinculación mencionada en el hecho de que el objeto social de la entidad se base precisamente en el manejo de los datos, sino en que para el desarrollo de ese objeto social sea habitual el citado manejo (e.g. el objeto social de una empresa del sector eléctrico no está relacionado con el tratamiento de datos, pero dicho tratamiento es necesario para el cumplimiento de dicho objeto social)[37], coinvirtiendo esta agravante en común a la mayoría de las resoluciones sancionadoras de la AEPD.

d) Finalmente, la AEPD se pronuncia en sus resoluciones acerca de las posibles atenuantes invocadas por los responsables, si bien, como regla general, desestima su aplicación al caso.

Así, la AEPD no aprecia el **grado de cooperación** del responsable o del encargado con la autoridad de control para subsanar la infracción y mitigar los posibles efectos adversos de la

[36] Resoluciones de los Procedimientos núm. PS/00677/2022, PS/00002/2023, PS/00020/2023, PS/00084/2023, PS/00145/2023, PS/00221/2023 y PS/00291/2023.
[37] Resoluciones de los Procedimientos núm. PS/00002/2023, PS/00145/2023 y PS/00221/2023.

infracción, al considerar que esta conducta no es espontánea, sino que procede el cumplimiento de una obligación explícita prevista en el artículo 33 del RGPD.

En cuanto a la implementación de **medidas adecuadas para mitigar los perjuicios sufridos por los interesados**, se aprecia excepcionalmente, por ejemplo, en caso en que se materialice a través de definición de un plan de auditorías que abarque todas las entidades de la organización sujetas a la normativa aplicable.[38]

Igualmente, la AEPD considera como un factor atenuante la ausencia de reclamaciones por parte de terceros, al considerar que cuando no se presentan quejas o denuncias ante la AEPD por parte de los afectados, se entiende que el impacto real del incidente ha sido reducido o prácticamente nulo[39].

La AEPD no aprecia que la **ausencia de un beneficio económico** derivado de la infracción pueda valorarse como un factor que justifique una reducción de la sanción, al entender que esta circunstancia únicamente podría considerarse una agravante en caso de existencia de beneficios.

Finalmente, la AEPD tampoco valora el **coste** asumido por la organización para mitigar los efectos del incidente de seguridad, al considerar que las medidas adoptadas tras el incidente deberían haber sido implementadas con anterioridad para garantizar un nivel adecuado de seguridad en función del riesgo[40]. En relación con este punto, es importante tener en cuenta que hay ocasiones en las que la AEPD ha considerado que se han aplicado suficientes medidas como para desestimar una reclamación y archivar las actuaciones[41]. En estos casos, se valora la existencia de medidas de seguridad previas a la brecha, la diligencia en la respuesta ante el incidente, la notificación a las autoridades competentes en tiempo y forma, así como la comunicación efectiva a los afectados. También se tiene en cuenta si hubo un impacto real sobre los derechos y libertades de las personas y si se implementaron medidas adicionales para reforzar la seguridad y prevenir futuras incidencias. Cuando se verifica que el responsable ha actuado de manera proporcional y conforme a la normativa vigente, la AEPD puede considerar que no se ha producido una vulneración sancionable, procediendo al archivo de la reclamación.

VII.- DECISIONES DE OTRAS AUTORIDADES DE PROTECCIÓN DE DATOS DEL EEE

Las distintas autoridades de protección de datos en los Estados miembros han sido también particularmente activas en lo referente a la investigación e imposición de sanciones como consecuencia de la existencia de brechas de seguridad. Entre las resoluciones más destacadas cabe hacer referencia a las siguientes:

La autoridad de protección de datos de Irlanda impuso tres sanciones, por importes totales de 265, 91 y 17 millones de euros a una importante red social[42], siendo relevante destacar que, en

[38] Procedimiento núm. E/09159/2020.

[39] Procedimiento núm. E/09159/2020.

[40] Resoluciones de los Procedimientos núm. PS/00084/2023, PS/00145/2023 y PS/00221/2023.

[41] Resolución del Procedimiento núm. E/09159/2020, accesible en: www.aepd.es/documento/e-09159-2020.pdf.

[42] La primera de ellas, como consecuencia de una infracción de los principios de privacidad desde el diseño y por defecto, al. Detectarse que los datos de 533 millones de usuarios eran accesibles en una plataforma de hackers. La

ambos casos, se produjo la tramitación del procedimiento coordinado, al que se ha hecho referencia en el punto 2 del apartado III de este informe. Asimismo, esta autoridad ha sido activa en el sector financiero, imponiendo una sanción de 750.000 euros a una entidad financiera como consecuencia del acceso no autorizado a los datos bancarios de sus clientes así como en el sector sanitario, imponiendo a una entidad titular de una red de centros sanitarios una sanción de 460.000 euros[43].

Por su parte, la autoridad italiana impuso una sanción de 79.1 millones de euros al principal suministrador eléctrico del país[44], y otra multa de 27.8 millones de euros al principal operador de telefonía móvil[45]. Asimismo, se impuso una sanción por importe de 15 millones a un importante motor de inteligencia artificial, dado que los usuarios visualizaban los historiales de títulos de chat de otros usuarios del servicio en lugar del suyo.

Asimismo, la autoridad británica de protección de datos impuso una sanción de 20.45 millones de euros a una importante cadena hotelera como consecuencia de una brecha de seguridad, no detectada durante un período prolongado de tiempo, que afectó, en particular, a los datos de las tarjetas de crédito de sus clientes.

La autoridad de protección de datos de Suecia sancionó con 3 millones de euros a una entidad aseguradora[46], imponiendo asimismo una sanción de 1.3 millones de euros a una entidad bancaria[47].

Finalmente, la Autoridad Polaca de Protección de Datos impuso a una entidad dedicada al marketing una sanción de 1.08 millones de euros[48], siendo relevante indicar que la sanción se impone por no supervisar adecuadamente la actuación de su encargado del tratamiento, que también fue sancionado.

Junto con las resoluciones adoptadas por estas autoridades, la práctica totalidad de ellas han dictado diversas resoluciones, con multas cuantiosas, relacionadas con las brechas de seguridad

---

segunda, fue consecuencia del hecho de mantener en texto plano las credenciales de acceso de sus usuarios. Finalmente, la tercera trae causa de una investigación relacionada con la notificación de doce brechas de seguridad producidas en un plazo de seis meses, no siendo la entidad capaz de probar que había adoptado medidas técnicas y organizativas de seguridad apropiadas para proteger los datos de los usuarios de la Unión Europea.

[43] Por un supuesto en que la misma sufrió un ataque de ransomware en el que se accedió a datos personales que fueron alterados y destruidos afectando a 70.000 personas, de las cuales 2.500 resultaron permanentemente afectadas.

[44] Entre otras cosas, por no mantener medidas de seguridad que permitieron el acceso malicioso a los datos de sus clientes para la realización de acciones comerciales por terceros no autorizados.

[45] Al ponerse de relieve algunos desajustes entre los sistemas que procesan los datos personales de los clientes, tales como provocar, por ejemplo, la atribución incorrecta de líneas telefónicas a los sujetos a cuyo nombre estaba registrado o la asociación incorrecta entre los sujetos a cuyo nombre están registradas y los datos de contacto utilizados por la Sociedad.

[46] Al constatarse que era posible el acceso por terceros a los datos personales de los 650.000 clientes de la compañía durante el período comprendido entre octubre de 2018 y febrero de 2021, incluyendo datos de salud e información financiera, entre otros.

[47] Dado que había utilizado en su sitio web y aplicación los denominados metapíxeles, que provocaban la transmisión a una red social de datos personales como valores mobiliarios y números de cuenta durante un período prolongado de tiempo.

[48] El encargado había permitido la creación de una copia de la base de datos de los clientes del responsable por parte de personas no autorizadas para ello.

de datos personales, pudiendo hacerse referencia en especial a las adoptadas por las autoridades de Croacia, Austria, Países Bajos, Noruega, Finlandia o Grecia.

En conjunto, la tendencia en Europa muestra un endurecimiento de las medidas sancionadoras en caso de brechas de seguridad, con un enfoque cada vez más estricto desde la perspectiva de la protección de los datos personales, que se manifiesta en la exigencia de mayores niveles de seguridad para evitar incidentes que comprometan la privacidad de los ciudadanos.

***