GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29

17/ES

WP 253

Directrices sobre la aplicación y la fijación de multas administrativas a efectos del Reglamento 2016/679

Adoptadas el 3 de octubre de 2017

El Grupo de Trabajo se creó de conformidad con el artículo 29 de la Directiva 95/46/CE. Se trata de un órgano consultivo independiente de la UE en materia de protección de datos e intimidad. Sus funciones se describen en el artículo 30 de la Directiva 95/46/CE y en el artículo 15 de la Directiva 2002/58/CE.

De su secretaría se ocupa la Dirección C (Derechos Fundamentales y Ciudadanía de la Unión) de la Dirección General de Justicia de la Comisión Europea, B-1049, Bruselas, Bélgica, Oficina n.º MO-59 03/075.

Sitio web: http://ec.europa.eu/justice/data-protection/index_en.htm

EL GRUPO DE TRABAJO RELATIVO A LA PROTECCIÓN DE LAS PERSONAS EN LO QUE RESPECTA AL

TRATAMIENTO DE DATOS PERSONALES

creado por la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995,

vistos los artículos 29 y 30 de dicha Directiva,

visto su Reglamento interno,

HA ADOPTADO LAS PRESENTES DIRECTRICES:

Índice:

I. Introducción

La UE ha llevado a cabo una reforma exhaustiva de la normativa que regula la protección de datos en Europa. Dicha reforma se asienta en varios pilares (componentes fundamentales): normas coherentes, procedimientos simplificados, acciones coordinadas, participación de los usuarios, información más efectiva y poderes coercitivos más contundentes.

Los responsables y los encargados del tratamiento de los datos han ampliado sus responsabilidades para garantizar la protección efectiva de los datos personales de las personas físicas. Las autoridades de control están facultadas para garantizar la defensa de los principios del Reglamento general de protección de datos (en lo sucesivo, el «Reglamento»), así como los derechos de las personas físicas de que se trate conforme a la letra y el espíritu del Reglamento.

Una ejecución coherente de las normas sobre protección de datos es vital para un régimen armonizado de protección de datos. Las multas administrativas son un elemento esencial del nuevo régimen de ejecución introducido por el Reglamento, puesto que constituyen una parte importante de los instrumentos de ejecución de que disponen las autoridades de control, junto con el resto de las medidas previstas en el artículo 58.

La finalidad del presente documento es que las autoridades de control lo utilicen para garantizar una mejora de la aplicación y ejecución del Reglamento y expresa su entendimiento común de las disposiciones del artículo 83 del Reglamento, así como su interrelación con los artículos 58 y 70 y sus correspondientes considerandos.

En particular, de acuerdo con el artículo 70, apartado 1, letra e), el Comité Europeo de Protección de Datos (en lo sucesivo, el «Comité») está facultado para emitir directrices, recomendaciones y buenas prácticas a fin de promover la aplicación coherente del presente Reglamento, y el artículo 70, apartado 1, letra k), especifica la formulación de directrices relativas a la fijación de multas administrativas.

Estas Directrices no son exhaustivas, ni proporcionan explicaciones sobre la diferencia entre los sistemas de Derecho administrativo, civil o penal en lo tocante a la imposición de sanciones administrativas en general.

Al objeto de lograr un planteamiento coherente de la imposición de multas administrativas que refleje adecuadamente todos los principios de las presentes directrices, el Comité ha consensuado un entendimiento común de los criterios de evaluación previstos en el artículo 83, apartado 2, del Reglamento, y por lo tanto, el Comité y las autoridades de control nacionales se comprometen a utilizar estas Directrices como enfoque común.

II. Principios

Una vez que se ha determinado que existe una infracción del Reglamento a partir de la apreciación de los hechos del caso, la autoridad de control competente debe identificar las medidas correctivas más apropiadas para abordar dicha infracción. Las disposiciones del artículo 58, apartado 2, letras b) a j)[1], señalan las herramientas que las autoridades de control pueden utilizar para abordar el incumplimiento de un responsable o un encargado del tratamiento. Al ejercer estos poderes, las autoridades de control deben observar los siguientes principios:

1. La infracción del Reglamento debe dar lugar a la imposición de «sanciones equivalentes».

El concepto de «equivalencia» es esencial a la hora de determinar el alcance de las obligaciones de las autoridades de control para garantizar la coherencia en su uso de los poderes correctivos con arreglo al artículo 58, apartado 2, en general, y la aplicación de multas administrativas en particular[2].

*Para garantizar un nivel uniforme y elevado de protección de las personas físicas y eliminar los obstáculos a la circulación de datos personales dentro de la Unión**, el nivel de protección de los derechos y libertades de las personas físicas por lo que se refiere al tratamiento de dichos datos debe ser equivalente** en todos los Estados miembros* (considerando 10). El considerando 11 aclara el hecho de que un nivel equivalente de protección de los datos personales en la Unión exige, entre otras cosas, «*que en los Estados miembros se reconozcan poderes equivalentes para supervisar y garantizar el cumplimiento de las normas relativas a la protección de los datos de carácter personal y las infracciones se castiguen con sanciones equivalentes*». Asimismo, la imposición de sanciones equivalentes en todos los Estados miembros y la cooperación efectiva entre las autoridades de control de distintos Estados miembros se consideran una forma de «*evitar divergencias que dificulten la libre circulación de datos personales dentro del mercado interior*», de conformidad con el considerando 13 del Reglamento.

El Reglamento establece una base más sólida que la Directiva 95/46/CE para lograr un mayor grado de coherencia, puesto que este es directamente aplicable en los Estados miembros. Aunque las autoridades de control actúan con «total independencia» (artículo 52) con respecto a los Gobiernos nacionales, los responsables y los encargados del tratamiento deben cooperar «*con el fin de garantizar la coherencia en la aplicación y ejecución del presente Reglamento*» [artículo 57, apartado 1, letra g)].

El Reglamento exige una mayor coherencia que la Directiva 95/46/CE en la imposición de sanciones. En casos transfronterizos, la coherencia se logrará principalmente mediante el mecanismo de cooperación (ventanilla única) y, en parte, mediante el mecanismo de coherencia previsto en el nuevo Reglamento.

En casos nacionales contemplados por el Reglamento, las autoridades de control aplicarán estas directrices con espíritu de cooperación, conforme al artículo 57, apartado 1, letra g), y el artículo 63, con el fin de garantizar la coherencia en la aplicación y ejecución del Reglamento. Aunque las

[1] El artículo 58, apartado 2, establece que se podrá sancionar con una advertencia cuando las «operaciones de tratamiento previstas puedan infringir lo dispuesto en el presente Reglamento». En otras palabras, de darse el caso contemplado en la disposición, la infracción del Reglamento no se ha producido aún.

[2] Aunque los ordenamientos jurídicos de algunos países de la UE no permiten las multas administrativas establecidas en el Reglamento, las normas sobre multas administrativas se pueden aplicar en dichos Estados miembros siempre que tal aplicación tenga un efecto equivalente a las multas administrativas impuestas por las autoridades de control (considerando 151). Los tribunales están sujetos al Reglamento, pero no están sujetos a estas Directrices del Comité.

autoridades de control son independientes a la hora de seleccionar las medidas correctivas previstas en el artículo 58, apartado 2, dichas autoridades deben evitar la elección de medidas correctivas distintas en casos similares.

Este mismo principio se aplica cuando dichas medidas correctivas se impongan en forma de multas.

2. Al igual que todas las medidas correctivas seleccionadas por las autoridades de control, las multas administrativas deben ser «efectivas, proporcionadas y disuasorias».

Como todas las medidas correctivas en general, las multas administrativas deben responder adecuadamente a la naturaleza, la gravedad y las consecuencias de la violación, y las autoridades de control deben evaluar todos los hechos del caso de una manera coherente y objetivamente justificada. La evaluación de lo que es efectivo, proporcionado y disuasorio en cada caso también deberá reflejar el objetivo perseguido por la medida correctiva seleccionada, ya sea restablecer el cumplimiento de la normativa o castigar un comportamiento ilícito (o ambos).

Las autoridades de control deben identificar una medida correctiva que sea «*efectiva, proporcionada y disuasoria*» (artículo 83, apartado 1), tanto en casos nacionales (artículo 55) como en casos que impliquen el tratamiento transfronterizo de datos personales (según se define en el artículo 4, apartado 23).

Las presentes Directrices reconocen que la legislación nacional podrá establecer requisitos complementarios sobre el procedimiento de ejecución que las autoridades de control deberán cumplir. Estos requisitos pueden incluir, por ejemplo, notificaciones, formularios, plazos para presentar alegaciones, recurso, ejecución y pago[3].

No obstante, estos requisitos no deben obstaculizar en la práctica los principios de eficacia, proporcionalidad y disuasión.

La práctica que vayan acumulando las autoridades de control (sobre protección de datos, así como las enseñanzas extraídas de otros sectores reguladores) y la jurisprudencia al interpretar estos principios generarán una determinación más precisa de eficacia, proporcionalidad y disuasión.

Para imponer multas efectivas, proporcionadas y disuasorias, la autoridad de control debe utilizar la definición del concepto de empresa prevista por el TJUE a los efectos de la aplicación de los artículos 101 y 102 del TFUE, a saber, que el concepto de empresa **debe entenderse** como una unidad económica que puede estar formada por la sociedad matriz y todas las filiales participantes. De acuerdo con el Derecho y la jurisprudencia de la UE[4], una empresa debe ser entendida como una unidad económica que lleva a cabo actividades comerciales/económicas, con independencia de la persona jurídica de que se trate (considerando 150).

[3] A modo de ejemplo, el marco constitucional y el proyecto de legislación de protección de datos de Irlanda disponen que ha de adoptarse una decisión formal sobre el hecho de la infracción en sí misma, que se comunica a las partes pertinentes, antes de evaluar la magnitud de las sanciones. La decisión sobre el hecho de la infracción en sí misma no se puede revisar durante la evaluación de la magnitud de las sanciones.

[4] La definición encontrada en la jurisprudencia del TJUE es: «el concepto de empresa comprende cualquier entidad que ejerza una actividad económica con independencia del estatuto jurídico de dicha entidad y de su modo de financiación» (véase la sentencia de 23 de abril de 1991, Höfner y Elser, C-41/90, EU:C:1991:161, apartado 21). «Debe entenderse que el concepto de empresa designa una unidad económica desde el punto de vista del objeto del acuerdo de que se trate, aunque, desde el punto de vista jurídico, esta unidad económica esté constituida por varias personas físicas o jurídicas» (véase la sentencia de 14 de diciembre de 2006, Confederación Española de Empresarios de Estaciones de Servicio, C-217/05, EU:C:2006:784, apartado 40)

3. La autoridad de control competente realizará una evaluación «de cada caso individual».

Las multas administrativas podrán imponerse como respuesta a un amplio abanico de infracciones. El artículo 83 del Reglamento prevé un planteamiento armonizado respecto de las violaciones de las obligaciones citadas expresamente en los apartados 4 a 6. La legislación del Estado miembro puede hacer extensiva la aplicación del artículo 83 a las autoridades y los órganos públicos establecidos en dicho Estado miembro. Asimismo, la legislación del Estado miembro puede consentir o incluso prescribir la imposición de una multa por la infracción de disposiciones distintas de las citadas en el artículo 83, apartados 4 a 6.

El Reglamento exige la evaluación de cada caso individual[5]. El artículo 83, apartado 2, es el punto de partida para dicha evaluación individual. Dicho apartado reza «*[a]l decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente en cuenta [...]*». En consecuencia, y también a la luz del considerando 148[6], la autoridad de control tiene la responsabilidad de seleccionar las medidas más apropiadas. En los casos citados en el artículo 83, apartados 4 a 6, esta selección **debe** comprender la consideración de todas las medidas correctivas, que abarcaría la consideración de la imposición de la multa administrativa adecuada, bien acompañada de una medida correctiva prevista en el artículo 58, apartado 2, o bien en solitario.

Las multas son herramientas importantes que las autoridades de control deben utilizar en las circunstancias apropiadas. Se insta a las autoridades de control a aplicar un planteamiento ponderado y equilibrado en su uso de las medidas correctivas, al objeto de lograr una reacción efectiva, disuasoria y proporcionada a la violación. La idea es no utilizar las multas como último recurso ni desincentivar su imposición, pero tampoco usarlas de un modo que devalúe su eficacia como herramienta.

[5] Además de la aplicación de los criterios del artículo 83, existen otras disposiciones que refuerzan la base de este planteamiento, como:

- considerando 141 «*La investigación abierta a raíz de una queja debe llevarse a cabo, bajo control judicial, en la medida en que sea adecuada en el caso específico*».
- considerando 129 «*Los poderes de las autoridades de control deben ejercerse de conformidad con garantías procesales adecuadas establecidas en el Derecho de la Unión y los Estados miembros, de forma imparcial, equitativa y en un plazo razonable*». *En particular, toda medida debe ser adecuada, necesaria y proporcionada con vistas a garantizar el cumplimiento del presente Reglamento, teniendo en cuenta las circunstancias de cada caso concreto...*».
- artículo 57, apartado 1, letra f) «*tratar las reclamaciones presentadas por un interesado o por un organismo, organización o asociación de conformidad con el artículo 8, e investigar, en la medida oportuna, el motivo de la reclamación*».

[6] «*A fin de reforzar la aplicación de las normas del presente Reglamento, cualquier infracción de este debe ser castigada con sanciones, incluidas multas administrativas, con carácter adicional a medidas adecuadas impuestas por la autoridad de control en virtud del presente Reglamento, o en sustitución de estas. En caso de infracción leve, o si la multa que probablemente se impusiera constituyese una carga desproporcionada para una persona física, en lugar de sanción mediante multa puede imponerse un apercibimiento. Debe no obstante prestarse especial atención a la naturaleza, gravedad y duración de la infracción, a su carácter intencional, a las medidas tomadas para paliar los daños y perjuicios sufridos, al grado de responsabilidad o a cualquier infracción anterior pertinente, a la forma en que la autoridad de control haya tenido conocimiento de la infracción, al cumplimiento de medidas ordenadas contra el responsable o encargado, a la adhesión a códigos de conducta y a cualquier otra circunstancia agravante o atenuante. La imposición de sanciones, incluidas las multas administrativas, debe estar sujeta a garantías procesales suficientes conforme a los principios generales del Derecho de la Unión y de la Carta, entre ellas el derecho a la tutela judicial efectiva y a un proceso con todas las garantías*».

Cuando esté facultado con arreglo al artículo 65 del Reglamento, el Comité adoptará una decisión vinculante en caso de diferencias entre autoridades de control relacionadas en particular con la determinación de la existencia de una infracción. Cuando la objeción pertinente y motivada plantee la cuestión de la conformidad de la medida correctiva con el RGPD, la decisión del Comité también tratará cómo se observan los principios de eficacia, proporcionalidad y disuasión en la multa administrativa propuesta en el proyecto de decisión de la autoridad de control competente. La orientación del Comité sobre la aplicación del artículo 65 del Reglamento se comunicará por separado para ofrecer más información sobre el tipo de decisión a adoptar por este.

4. Un planteamiento armonizado de las multas administrativas en el ámbito de la protección de datos requiere la participación activa y el intercambio de información entre las autoridades de control.

Las presentes Directrices reconocen que, para algunas autoridades de control nacionales, las competencias de imposición de multas constituyen una novedad en el ámbito de la protección de datos, lo que plantea numerosos problemas en términos de recursos, organización y procedimiento. Cabe destacar que las decisiones en las que las autoridades de control ejerzan las competencias de imposición de multas conferidas estarán sujetas a recurso ante los tribunales nacionales.

Las autoridades de control cooperarán entre sí y, si procede, con la Comisión Europea a través de los mecanismos de cooperación previstos en el Reglamento, para fomentar intercambios de información formales e informales, como por ejemplo a través de talleres periódicos. La cooperación se centraría en su experiencia y práctica en la aplicación de las competencias de imposición de multas para lograr, en última instancia, una mayor coherencia.

Este intercambio de información proactivo, junto con la jurisprudencia que vaya surgiendo sobre el uso de estas competencias, puede desembocar en la revisión de los principios o los detalles concretos de las presentes Directrices.

III. Criterios de evaluación del artículo 83, apartado 2

El artículo 83, apartado 2, establece una lista de criterios que las autoridades de control deben usar para determinar si ha de imponerse una multa y la cuantía de la misma. No recomienda una evaluación reiterada del mismo criterio, sino una evaluación que tenga en cuenta todas las circunstancias de cada caso individual, según lo contemplado en el artículo 83[7].

Las conclusiones de la primera fase de la evaluación pueden utilizarse en la segunda parte con relación a la cuantía de la multa, evitando así la necesidad de utilizar dos veces los mismos criterios.

En esta sección se ofrecen orientaciones a las autoridades de control sobre cómo interpretar los hechos individuales del caso a la luz de los criterios del artículo 83, apartado 2.

a) la naturaleza, gravedad y duración de la infracción

Casi todas las obligaciones de los responsables y los encargados del tratamiento previstas en el Reglamento se clasifican de acuerdo con su **naturaleza** en las disposiciones del artículo 83, apartados 4 a 6. Al establecer dos cuantías máximas distintas de multas administrativas (10 000 000 y 20 000 000 EUR), el Reglamento ya indica que la violación de determinadas disposiciones del mismo puede ser más grave que la violación de otras disposiciones. Sin embargo, mediante la evaluación de los hechos del caso a la luz de los criterios generales previstos en el artículo 83, apartado 2, la autoridad de control competente puede decidir que en un caso concreto es más o menos necesario imponer una medida correctiva en forma de multa. Cuando se elige una multa como única medida correctiva o como una entre varias medidas correctivas apropiadas, se aplicará el sistema de niveles del Reglamento (artículo 83, apartados 4 a 6) para identificar la multa máxima que se puede imponer con arreglo a la naturaleza de la infracción en cuestión.

En el considerando 148 se presenta la noción de «infracciones leves». Dichas infracciones pueden constituir violaciones de una o varias disposiciones del Reglamento citadas en el artículo 83, apartados 4 o 5. No obstante, la evaluación de los criterios previstos en el artículo 83, apartado 2, puede dar lugar a que la autoridad de control estime, por ejemplo, que en las circunstancias concretas del caso la violación no entraña un riesgo importante para los derechos de los interesados y no afecta a la esencia de la obligación en cuestión. En tales casos, la multa puede ser sustituida (aunque no siempre) por un apercibimiento.

El considerando 148 no obliga a la autoridad de control a sustituir siempre una multa por un apercibimiento en caso de infracción leve («*en lugar de sanción mediante multa puede imponerse un apercibimiento*»), sino que más bien ofrece esa posibilidad, tras una evaluación concreta de todas las circunstancias del caso.

El considerando 148 ofrece esta misma posibilidad de sustituir una multa por un apercibimiento en el caso de que el responsable del tratamiento de los datos sea una persona física y la multa que probablemente se impusiera constituyese una carga desproporcionada. El punto de partida es que la autoridad de control debe evaluar si, a la luz de todas las circunstancias del caso, se requiere la imposición de una multa. Si se determina que debe imponerse una multa, la autoridad de control debe evaluar si la multa que debe imponerse constituiría una carga desproporcionada para una persona física.

En el Reglamento no se estipulan cuantías concretas para infracciones concretas, solo un máximo (cuantía máxima). Esto puede indicar la existencia de un grado relativo más bajo de gravedad para una

[7] La evaluación de la sanción a aplicar puede llevarse a cabo por separado después de evaluar si se ha producido una infracción con arreglo a las normas procesales nacionales derivadas de las normas constitucionales en algunos países. Por lo tanto, esto puede limitar el contenido y el nivel de detalle del proyecto de decisión emitido por la autoridad de control principal en dichos países.

violación de las obligaciones citadas en el artículo 83, apartado 4, en comparación con las previstas en el artículo 83, apartado 5. No obstante, la reacción efectiva, proporcionada y disuasoria ante una violación del artículo 83, apartado 5, dependerá de las circunstancias del caso.

Cabe destacar que las violaciones del Reglamento que por su naturaleza pudieran englobarse en la categoría de «hasta 10 000 000 EUR o hasta el 2 % del volumen de negocio total anual global», según lo previsto en el artículo 83, apartado 4, podrían terminar englobándose en una categoría superior (20 000 000 EUR) en determinadas circunstancias. Probablemente, este sería el caso si dichas violaciones hubieran sido previamente abordadas en una resolución de la autoridad de control, una resolución[8] que el responsable o el encargado del tratamiento no hubieran acatado[9] (artículo 83, apartado 6). Las disposiciones del Derecho nacional pueden tener en la práctica un efecto sobre esta evaluación[10]. La naturaleza de la infracción, pero también «*el alcance o propósito de la operación de tratamiento de que se trate, así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido*» serán indicativos de la **gravedad** de la infracción. La comisión de varias infracciones distintas en un caso individual concreto permite a la autoridad de control aplicar las multas administrativas a un nivel que sea efectivo, proporcionado y disuasorio dentro de los límites de la infracción más grave. Por lo tanto, si se detecta una infracción de los artículos 8 y 12, la autoridad de control puede aplicar las medidas correctivas previstas en el artículo 83, apartado 5, correspondientes a la categoría de la infracción más grave, es decir, el artículo 12. Esta directriz concreta no aborda más detalles en esta fase (ya que la labor detallada de cálculo se trataría en una posible fase posterior de esta directriz).

Los siguientes factores deben evaluarse de manera combinada, es decir, el número de interesados junto con el posible impacto sobre ellos.

---

[8] Los poderes previstos en el artículo 58, apartado 2, son:

- ordenar al responsable o encargado del tratamiento que atiendan las solicitudes de ejercicio de los derechos del interesado en virtud del presente Reglamento;
- ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado;
- ordenar al responsable del tratamiento que comunique al interesado las violaciones de la seguridad de los datos personales;
- imponer una limitación temporal o definitiva del tratamiento, incluida su prohibición;
- ordenar la rectificación o supresión de datos personales o la limitación de tratamiento con arreglo a los artículos 16, 17 y 18 y la notificación de dichas medidas a los destinatarios a quienes se hayan comunicado datos personales con arreglo a al artículo 17, apartado 2, y al artículo 19;
- ordenar al organismo de certificación que retire una certificación emitida con arreglo a los artículos 42 y 43, u ordenar al organismo de certificación que no se emita una certificación si no se cumplen o dejan de cumplirse los requisitos para la certificación;
- ordenar la suspensión de los flujos de datos hacia un destinatario situado en un tercer país o hacia una organización internacional.

[9] La aplicación del artículo 83, apartado 6, ha de tener necesariamente en cuenta el Derecho procesal nacional aplicable. El Derecho nacional determina cómo se emite una orden, cómo se notifica, su fecha de entrada en vigor y si existe un período de gracia para el cumplimiento. Ha de tenerse especialmente en cuenta el efecto de un recurso sobre la ejecutoriedad de una resolución.

[10] Las disposiciones legales relativas a la prescripción pueden tener el efecto de que una resolución anterior de la autoridad de control deje de tenerse en cuenta debido al tiempo transcurrido desde la emisión de la misma. En algunas jurisdicciones, las normas determinan que una vez transcurrido el período de prescripción con respecto a una resolución no se pueden imponer multas por el incumplimiento de dicha resolución en virtud del artículo 83, apartado 6. Dependerá de cada autoridad de control de cada jurisdicción determinar cómo les afectarán estos impactos.

El número de interesados debe evaluarse para determinar si se trata de un hecho aislado o sintomático de una violación más sistemática o de una falta de rutinas adecuadas. Esto no quiere decir que los hechos aislados no deban sancionarse, ya que un hecho aislado podría afectar a muchos interesados. Dependiendo de las circunstancias del caso, esto guardará relación con, por ejemplo, el número total de solicitantes de la base de datos en cuestión, el número de usuarios de un servicio, el número de clientes o la población del país, según proceda.

El propósito del tratamiento también debe evaluarse. El dictamen del Grupo de Trabajo 29 sobre la «limitación de finalidad»[11] analizó previamente los dos componentes principales de este principio en la legislación de protección de datos: finalidad y uso compatible. A la hora de evaluar la finalidad de la operación de tratamiento en el contexto del artículo 83, apartado 2, las autoridades de control deben analizar la medida en que la operación de tratamiento respalda los dos componentes principales de este principio[12]. En determinadas situaciones, la autoridad de control podría considerar necesario profundizar en el análisis de la finalidad de la operación de tratamiento en sí en el análisis del artículo 83, apartado 2.

Si los interesados han sufrido **daños y perjuicios**, ha de tenerse en cuenta el nivel de los mismos. El tratamiento de datos personales puede generar riesgos para los derechos y las libertades individuales, tal y como se ilustra en el considerando 75:

> «*Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo; en los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales; en los casos en los que los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas; en los casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales; en los casos en los que se traten datos personales de personas vulnerables, en particular niños; o en los casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados*».

Si se han sufrido o es probable que se sufran daños y perjuicios debido a la infracción del Reglamento, la autoridad de control debe tener esto en cuenta a la hora de seleccionar la medida correctiva, aunque la autoridad de control carezca de competencias para otorgar la indemnización específica por los daños y perjuicios sufridos.

La imposición de una multa no depende de la capacidad de la autoridad de control de determinar una relación causal entre la violación y la pérdida material (véase, por ejemplo, el artículo 83, apartado 6).

---

[11] WP 203, Dictamen 03/2013 sobre limitación de finalidad, disponible (en inglés) en: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

[12] Véase también WP 2017, Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE, página 24, sobre la pregunta: «¿Qué convierte a un interés en «legítimo» o «ilegítimo»?»

La duración de la infracción puede ser indicativa de:

a) acto premeditado del responsable del tratamiento de los datos, o

b) no adopción de las medidas preventivas apropiadas, o

c) incapacidad para implantar las medidas organizativas o técnicas exigidas.

b) la intencionalidad o negligencia en la infracción

En general, «intención» implica conocimiento y voluntariedad en relación con las características de un delito, mientras que «involuntario» significa que no hubo intención de cometer la infracción, aunque el responsable o el encargado del tratamiento incumplieran la obligación de cautela que exige la ley.

Por regla general, se considera que las violaciones intencionadas, que demuestran desprecio por las disposiciones de la ley, son más graves que las violaciones involuntarias y, por lo tanto, es más probable que justifiquen la imposición de una multa administrativa. Las conclusiones pertinentes sobre voluntariedad o negligencia se extraerán identificando los elementos objetivos de la conducta recabados gracias a los hechos del caso. Asimismo, la jurisprudencia y la práctica que vayan surgiendo en el ámbito de la protección de datos en virtud de la aplicación del Reglamento serán ilustrativas de circunstancias que indiquen umbrales más claros para evaluar si una violación fue intencionada.

Podrían considerarse circunstancias indicativas de violaciones intencionadas el tratamiento ilegítimo autorizado explícitamente por los superiores del responsable del tratamiento, o a pesar de los consejos del delegado de protección de datos o haciendo caso omiso a las políticas existentes, por ejemplo, la obtención y el tratamiento de datos sobre empleados de un competidor con la intención de desacreditarlo en el mercado.

Otros ejemplos podrían ser:

- la modificación de datos personales para ofrecer una impresión engañosa (positiva) sobre el cumplimiento de los objetivos; hemos sido testigos de esta conducta en el contexto de los objetivos de los tiempos de espera en hospitales
- el comercio de datos personales con fines de mercadotecnia, es decir, la venta de datos como «participación voluntaria» sin comprobar la opinión de los interesados sobre cómo deberían usarse sus datos o haciendo caso omiso a dicha opinión.

Otras circunstancias, como la falta de lectura y aceptación de las políticas existentes, errores humanos, la falta de comprobación de datos personales en la información publicada, la falta de aplicación de actualizaciones técnicas de un modo oportuno o la falta de adopción de políticas (y no solo su falta de aplicación) pueden ser indicativas de negligencia.

Las empresas deben ser responsables de adoptar las estructuras y los recursos adecuados a la naturaleza y la complejidad de su negocio. Por lo tanto, los responsables y los encargados del tratamiento no pueden legitimizar violaciones de la legislación de protección de datos alegando escasez de recursos. Las rutinas y la documentación de las actividades de tratamiento siguen un enfoque basado en los riesgos conforme al Reglamento.

Existen cuestiones poco claras que afectarán a la toma de decisiones relacionadas con la imposición o la no imposición de una medida correctiva, y es posible que la autoridad tenga que realizar una investigación más exhaustiva para verificar los hechos del caso y garantizar la consideración suficiente de todas las circunstancias particulares de cada caso individual.

c) cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados;

Los responsables y los encargados del tratamiento de los datos tienen la obligación de aplicar medidas técnicas y organizativas para garantizar un nivel de seguridad adecuado al riesgo, llevar a cabo evaluaciones de impacto relativas a la protección de datos y mitigar los riesgos para los derechos y las libertades individuales derivados del tratamiento de datos personales. Sin embargo, cuando se produce una violación y el interesado ha sufrido daños y perjuicios, la parte responsable debe hacer todo lo que esté a su alcance para paliar las consecuencias de la violación para los individuos de que se trate. La autoridad de control tendría en cuenta dicha conducta responsable (o la ausencia de ella) a la hora de seleccionar las medidas correctivas, así como en el momento de calcular la sanción a imponer en el caso concreto.

Aunque los factores agravantes y atenuantes son particularmente idóneos para adaptar la cuantía de una multa a las circunstancias particulares del caso, su importancia no debe subestimarse en la selección de la medida correctiva apropiada. En casos en los que la evaluación basada en otros criterios no termine de convencer a la autoridad de control sobre la idoneidad de una multa administrativa, como medida correctiva individual, o en combinación con otras medidas previstas en el artículo 58, dichas circunstancias agravantes o atenuantes pueden ayudar a seleccionar las medidas apropiadas inclinando la balanza a favor de lo que se considere más efectivo, proporcionado y disuasorio en el caso concreto.

Esta disposición actúa como una evaluación del grado de responsabilidad del responsable del tratamiento una vez cometida la infracción. Puede abarcar casos en los que el responsable o el encargado del tratamiento claramente no hayan mostrado una conducta imprudente/negligente, sino en los que hubieran hecho todo lo posible por corregir sus acciones una vez conocida la infracción.

La experiencia normativa acumulada por las autoridades de control en virtud de la Directiva 95/46/CE ha demostrado que puede ser adecuado mostrar cierto grado de flexibilidad para los responsables o los encargados del tratamiento de los datos que hayan admitido su infracción y asumido la responsabilidad de corregir o limitar el impacto de sus acciones. Aquí podrían incluirse ejemplos como (aunque esto no daría lugar a un planteamiento más flexible en todos los casos):

- contactar con otros responsables o encargados del tratamiento que podrían haber participado en una extensión del tratamiento, por ejemplo, si se ha compartido por error algún dato con terceros;
- adoptar una medida oportuna para poner fin a la infracción o evitar su expansión a un nivel o fase en la que dicha infracción hubiera tenido un impacto mucho más grave del que finalmente tuvo.

d) el grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 25 y 32;

El Reglamento ha introducido un nivel mucho mayor de rendición de cuentas del responsable del tratamiento de los datos en comparación con la Directiva 95/46/CE sobre protección de datos.

El grado de responsabilidad del responsable o el encargado del tratamiento evaluado en el contexto de la aplicación de una medida correctiva apropiada puede incluir:

- ¿El responsable del tratamiento ha aplicado medidas técnicas que se atienen a los principios de protección de datos desde el diseño y por defecto (artículo 25)?
- ¿El responsable del tratamiento ha aplicado medidas organizativas para dar cumplimiento a los principios de protección de datos desde el diseño y por defecto (artículo 25) en todos los niveles de la organización?
- ¿El responsable/encargado del tratamiento ha aplicado un nivel de seguridad apropiado (artículo 32)?

- ¿Se conocen y se han aplicado las rutinas/políticas de protección de datos pertinentes en el nivel apropiado de dirección de la organización? (artículo 24).

Los artículos 25 y 32 del Reglamento exigen que los responsables del tratamiento «*tengan en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas*». Más que ser una obligación de resultado, estas disposiciones introducen una obligación de medios, es decir, el responsable del tratamiento debe realizar las evaluaciones necesarias y llegar a las conclusiones apropiadas. Por tanto, la pregunta a la que la autoridad de control debe responder es en qué medida el responsable del tratamiento «hizo lo que podía esperarse que hiciera» habida cuenta de la naturaleza, los fines o el ámbito de la operación de tratamiento, a la luz de las obligaciones que le impone el Reglamento.

En esta evaluación, deben tenerse debidamente en cuenta los métodos o procedimientos de «buenas prácticas», de existir y aplicarse. También es importante tener en cuenta las normas del sector, así como los códigos de conducta de la profesión o el ámbito respectivos. Los códigos de buenas prácticas podrían indicar lo que se consideran prácticas comunes en el ámbito, así como el nivel de conocimientos sobre distintas formas de abordar problemas de seguridad habituales asociados al tratamiento.

Aunque el ideal a perseguir en general son las buenas prácticas, han de tenerse en cuenta las circunstancias especiales de cada caso individual a la hora de evaluar el grado de responsabilidad.

e) toda infracción anterior cometida por el responsable o el encargado del tratamiento;

Este criterio está previsto para evaluar la trayectoria de la entidad que comete la infracción. Las autoridades de control deben tener en cuenta que el alcance de la evaluación puede ser bastante amplio porque cualquier tipo de violación del Reglamento, aunque su naturaleza sea distinta de la investigada en ese momento por la autoridad de control, podría ser «pertinente» para la evaluación, ya que podría ser indicativo de un nivel general de conocimiento insuficiente o desprecio por las normas de protección de datos.

La autoridad de control debe evaluar:

- ¿El responsable o el encargado del tratamiento han cometido anteriormente la misma infracción?
- ¿El responsable o el encargado del tratamiento cometieron una infracción del Reglamento de la misma manera? (por ejemplo, como consecuencia de un conocimiento insuficiente de las rutinas existentes en la organización, o como consecuencia de una evaluación inadecuada del riesgo, por no responder de manera oportuna a las peticiones del interesado, por demorarse injustificadamente al responder a dichas peticiones, etc.).

f) el grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción;

El artículo 83, apartado 2, estipula que el grado de cooperación se tendrá «debidamente en cuenta» al decidir la imposición de una multa administrativa y su cuantía. El Reglamento no ofrece una respuesta precisa a la pregunta de cómo tener en cuenta los esfuerzos de los responsables y los encargados del tratamiento para remediar una infracción ya determinada por la autoridad de control. Asimismo, está claro que los criterios se aplicarían normalmente a la hora de calcular la cuantía de la multa a imponer.

Sin embargo, cuando la intervención del responsable del tratamiento haya tenido el efecto de impedir o paliar las consecuencias negativas sobre los derechos de las personas, esto también se tendrá en cuenta a la hora de seleccionar la medida correctiva proporcionada al caso individual.

Un ejemplo de un caso en el que podría ser relevante la consideración de la cooperación con la autoridad de control sería:

- ¿La entidad ha respondido de una forma concreta a las peticiones de la autoridad de control durante la fase de investigación en ese caso concreto, lo que ha limitado notablemente el impacto sobre los derechos de las personas?

Dicho esto, no sería apropiado tener en cuenta por añadidura la cooperación que la ley exige; por ejemplo, en todo caso se exige a la entidad permitir a la autoridad de control acceso a las instalaciones para realizar auditorías o inspecciones.

g) las categorías de los datos de carácter personal afectados por la infracción;

Algunos ejemplos de preguntas importantes que la autoridad de control podría tener que responder aquí, de ser apropiado para el caso, son:

- ¿La infracción afecta al tratamiento de categorías especiales de datos establecidas en los artículos 9 o 10 del Reglamento?
- ¿Los datos son directamente identificables o indirectamente identificables?
- ¿El tratamiento abarca datos cuya difusión provocaría daños y perjuicios inmediatos al individuo (no englobados en la categoría de los artículos 9 o 10)?

- ¿Los datos están directamente disponibles sin medidas técnicas de protección o están cifrados[13]?

h) la forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida;

Una autoridad de control podría tener conocimiento de la infracción como resultado de una investigación, reclamaciones, artículos de prensa, avisos anónimos o la notificación de un responsable del tratamiento de los datos. Según el Reglamento, el responsable del tratamiento tiene la obligación de notificar a la autoridad de control las violaciones de la seguridad de los datos personales. En los casos en los que el responsable se limite a cumplir esta obligación, dicho cumplimiento no se puede interpretar como un factor atenuante / mitigante. Asimismo, un responsable/encargado del tratamiento de los datos que no notificó dicha violación o que no notificó todos los detalles de la misma por no haber evaluado adecuadamente el alcance de la violación también podría merecer una sanción más grave por parte de la autoridad de control, es decir, es improbable que la suya se clasificara como una infracción leve.

i) cuando las medidas indicadas en el artículo 58, apartado 2, hayan sido ordenadas previamente contra el responsable o el encargado de que se trate en relación con el mismo asunto, el cumplimiento de dichas medidas;

Un responsable o encargado del tratamiento ya podría hallarse bajo la vigilancia de la autoridad de control para supervisar su cumplimiento tras haber cometido una infracción previa y cuando los contactos con el delegado de protección de datos, en caso de que existan, hayan sido importantes. Por lo tanto, la autoridad de control tendrá en cuenta los contactos previos.

Contrariamente a los criterios previstos en la letra e), estos criterios de evaluación solo persiguen recordar a las autoridades de control que consulten las medidas que han emitido previamente para el mismo responsable o encargado «*relativas al mismo asunto en relación con el tratamiento*».

j) la adhesión a códigos de conducta en virtud del artículo 40 o a mecanismos de certificación aprobados con arreglo al artículo 42;

Las autoridades de control tienen la obligación de «*controlar la aplicación del presente Reglamento y hacerlo aplicar*» [artículo 57, apartado 1, letra a)]. El responsable o encargado del tratamiento pueden utilizar la adhesión a códigos de conducta aprobados para demostrar el cumplimiento, de acuerdo con el artículo 24, apartado 3, el artículo 28, apartado 5, o el artículo 32, apartado 3.

En caso de violación de una de las disposiciones del Reglamento, la adhesión a un código de conducta aprobado podría indicar lo importante que es intervenir con una multa administrativa efectiva, proporcionada y disuasoria u otra medida correctiva de la autoridad de control. Según el artículo 40, apartado 4, los códigos de conducta aprobados contendrán «*mecanismos que permitan al organismo (de supervisión) efectuar el control obligatorio del cumplimiento de sus disposiciones*».

Cuando el responsable o el encargado del tratamiento se hayan atenido a un código de conducta aprobado, la autoridad de control podría darse por satisfecha si la comunidad encargada de administrar dicho código adopta una medida apropiada contra su miembro, por ejemplo, a través de los regímenes de supervisión y aplicación del propio código de conducta. Por lo tanto, la autoridad de control podría considerar que dichas medidas son lo suficientemente efectivas, proporcionadas y disuasorias en ese caso concreto sin necesidad de imponer medidas complementarias. Ciertas formas de sanciones de incumplimientos podrían realizarse a través del régimen de supervisión, con arreglo al artículo 41,

[13] No siempre debe considerarse un factor atenuante adicional que la violación solo concierna a datos indirectamente identificables o incluso pseudonimizados o cifrados. Para dichas violaciones, una evaluación general de los otros criterios podría dar pruebas buenas o moderadas de que debe imponerse una multa.

apartado 2, letra c), y el artículo 42, apartado 4, incluidas la suspensión o la exclusión del responsable o el encargado del procesamiento de que se trate de la comunidad del código. No obstante, las competencias del organismo de supervisión deben entenderse «*sin perjuicio de las funciones y los poderes de la autoridad de control competente*», lo que significa que la autoridad de control no tiene la obligación de tener en cuenta sanciones impuestas previamente correspondientes al régimen de autorregulación.

El incumplimiento de las medidas de autorregulación también podría revelar la negligencia o la conducta intencionada del responsable o el encargado del tratamiento.

k) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción.

La propia disposición ofrece ejemplos de otros elementos que podrían tenerse en cuenta a la hora de decidir la idoneidad de una multa administrativa por una infracción de las disposiciones previstas en el artículo 83, apartados 4 a 6.

La información sobre el beneficio obtenido como resultado de una violación puede ser especialmente importante para las autoridades de control, ya que la ganancia económica resultante de una infracción no se puede compensar con medidas que no tienen un componente pecuniario. Por lo tanto, el hecho de que el responsable del tratamiento se hubiera beneficiado de la infracción del Reglamento podría constituir una señal clara de que debe imponerse una multa.

IV. Conclusiones

Las reflexiones sobre las preguntas planteadas en la sección anterior ayudarán a las autoridades de control a determinar a partir de los hechos relevantes del caso los criterios más útiles para tomar una decisión sobre la imposición de una multa administrativa apropiada sumada a otras medidas previstas en el artículo 58 o en lugar de estas. Habida cuenta del contexto proporcionado por dicha evaluación, la autoridad de control determinará la medida correctiva más efectiva, proporcionada y disuasoria para responder a la violación.

El artículo 58 proporciona orientaciones sobre las medidas que podría seleccionar una autoridad de control, ya que las medidas correctivas en sí mismas son de naturaleza distinta y están previstas para la consecución de propósitos distintos. Algunas de las medidas contempladas en el artículo 58 podrían incluso ser acumulativas, logrando así una acción reguladora compuesta por más de una medida correctiva.

No siempre es necesario complementar la medida con el uso de otra medida correctiva. Por ejemplo: la eficacia o el efecto disuasorio de la intervención de la autoridad de control con la debida consideración de lo que es proporcionado en un caso concreto pueden lograrse a través de una multa exclusivamente.

En esencia, las autoridades deben restablecer el cumplimiento a través de las medidas correctivas de las que disponen. Asimismo, se exige a las autoridades de control que seleccionen el canal más apropiado para perseguir la acción reguladora. Por ejemplo, este podría comprender sanciones penales (en caso de que estas estuvieran disponibles a escala nacional).

La práctica de aplicar multas administrativas de forma coherente en la Unión Europea es un arte en evolución. Las autoridades de control deben adoptar medidas que actúen conjuntamente para mejorar la coherencia de forma continua. Este fin se puede lograr mediante intercambios regulares a través de talleres de tratamiento de casos u otras actividades que permitan la comparación de casos a nivel subnacional, nacional y transfronterizo. Se recomienda la creación de un subgrupo permanente vinculado a una parte pertinente del Comité para apoyar esta actividad continua.