Decisión 01/2020 relativa al conflicto planteado por el proyecto de decisión de la autoridad de control irlandesa en relación con Twitter International Company con arreglo al artículo 65, apartado 1, letra a) del RGPD

Adoptada el 9 de noviembre de 2020

Translations proofread by EDPB Members.

This language version has not yet been proofread.

Índice

El Comité Europeo de Protección de Datos

Vistos el artículo 63 y el artículo 65, apartado 1, letra a) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, 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 y por el que se deroga la Directiva 95/46/CE (en lo sucesivo, el «**RGPD**»)[1],

Visto el Acuerdo sobre el Espacio Económico Europeo y, en particular, su anexo XI y su Protocolo 37, modificado por la Decisión del Comité conjunto del EEE n.º 154/2018, de 6 de julio de 2018,[2]

Vistos los artículos 11 y 22 de su Reglamento interno[3],

Considerando lo siguiente:

(1) El principal cometido del Comité Europeo de Protección de Datos (en lo sucesivo, el «**CEPD**» o el «**Comité**») es garantizar la aplicación uniforme del RGPD en todo el EEE. A este fin, del artículo 60 del RGPD se deduce que la autoridad de control principal (en lo sucesivo la «**ACP**») cooperará con las restantes autoridades de control interesadas (en lo sucesivo las «**ACI**») en un intento de alcanzar un consenso, que la ACP y las ACI se intercambiarán toda la información pertinente, y que la ACP comunicará sin demoras, a las demás autoridades de control interesadas, la información pertinente a este respecto. La ACP presentará sin demoras un proyecto de decisión a las demás ACI a fin de recabar su dictamen al respecto y tendrá debidamente en cuenta sus puntos de vista.

(2) En caso de que cualquiera de las ACI formule una objeción pertinente y motivada («**OPM**») acerca del proyecto de decisión, conforme al artículo 4, apartado 24, y al artículo 60, apartado 4, del RGPD, y la ACP no tenga intención de seguir lo indicado en la OPM o estime que dicha objeción no es pertinente o no está motivada, la ACP someterá el asunto al mecanismo de coherencia contemplado en el artículo 63 del RGPD.

(3) Conforme al artículo 65, apartado 1, letra a), del RGPD, el CEPD adoptará una decisión vinculante en todos los asuntos referidos a las OPM, en particular si hay infracción del RGPD.

(4) La decisión vinculante del CEPD deberá ser aprobada por una mayoría de dos tercios de los miembros del CEPD en virtud del artículo 65, apartado 2, del RGPD, en combinación con el artículo 11, apartado 4, del Reglamento interno del CEPD, en un plazo de un mes a contar desde el momento en que el presidente y la autoridad de control competente hayan decidido que el expediente está completo. Este plazo se podrá prorrogar un mes más, si la complejidad del tema así lo exige, por decisión del presidente, por iniciativa propia o a petición de al menos un tercio de los miembros del CEPD.

(5) De conformidad con el artículo 65, apartado 3, del RGPD, cuando, a pesar de dicha prórroga, el CEPD no haya podido adoptar una decisión dentro del plazo, lo hará en un plazo de dos semanas tras la expiración de la prórroga, por mayoría simple de sus miembros.

---

[1] DO L 119, de 4.5.2016, p. 1.

[2] En la presente decisión, las referencias a los «Estados miembros» deben entenderse como referencias a los «Estados miembros del EEE». Las referencias a la «UE» deben entenderse, cuando proceda, como referencias al «EEE».

[3] Reglamento interno del CEPD, aprobado el 25 de mayo de 2018, conforme a su última modificación y adopción el 8 de octubre de 2020.

1 RESUMEN DEL CONFLICTO

1. Este documento contiene una decisión vinculante adoptada por el CEPD conforme al artículo 65, apartado 1, letra a) del RGPD. La decisión se refiere al conflicto surgido como consecuencia de un proyecto de decisión (en adelante el «**Proyecto de decisión**») adoptado por la autoridad de control irlandesa («Data Protection Comission», en adelante «**AC IE**» y en este contexto también la «**ACP**»), y las objeciones posteriores expresadas por una serie de ACI («Österreichische Datenschutzbehörde», en adelante «**AC AT**»; «Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit»[4], en adelante «**AC DE**»; «Datatilsynet», en adelante «**AC DK**»; «Agencia Española de Protección de Datos», en adelante «**AC ES**»; «Commission Nationale de l'Informatique et des Libertés», en adelante «**AC FR**»; «Nemzeti Adatvédelmi és Információszabadság Hatóság», en adelante «**AC HU**»; «Garante per la protezione dei dati personali», en adelante «**AC IT**»; «Autoriteit Persoonsgegevens», en adelante «**AC NL**»). El proyecto de decisión en cuestión se refiere a una «investigación por iniciativa propia» iniciada por la AC IE tras la **notificación de una violación de la seguridad de datos personales** el 8 de enero de 2019 («**la Violación**») por parte de Twitter International Company, una sociedad establecida en Dublín, Irlanda (en adelante «**TIC**»)[5].

2. La violación de la seguridad de los datos surgió como consecuencia de **un defecto en el código informático de Twitter**, debido al cual, si un usuario de un dispositivo Android cambiaba la dirección electrónica asociada a su cuenta de Twitter, los tuiteos («*tweets*») protegidos quedaban desprotegidos y, por lo tanto, accesibles a un público más amplio (y no solo a los seguidores del usuario), sin que el usuario tuviera conocimiento de ello[6]. El defecto lo descubrió el 26 de diciembre de 2018 un contratista externo que gestionaba el «*bug bounty programme*», que es un programa de recompensa para quien informe sobre errores[7].

3. Durante su investigación, Twitter descubrió que otras acciones de los usuarios también provocaban el mismo resultado involuntario. El defecto del código **se remontaba a un cambio de código efectuado el 4 de noviembre de 2014**[8].

4. TIC informó a la AC IE de que, en la medida en que ellos podían detectar, entre el 5 de septiembre de 2017 y el 11 de enero de 2019, **88 726 usuarios de la UE y del EEE se habían visto afectados** por este defecto. Twitter ha confirmado que el defecto se remonta al 4 de noviembre de 2014, pero también ha confirmado que solo puede identificar a los usuarios afectados a partir del 5 de septiembre de 2017, debido a la política de conservación aplicable a los registros[9]. En consecuencia, TIC reconoció la posibilidad de que el número de usuarios afectados por la violación de la seguridad pudiera ser mayor[10].

[4] La objeción por parte de la AC Hamburgo se presentó también en representación de «Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg», «Berliner Beauftragte für Datenschutz und Informationsfreiheit», «Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern», «Die Landesbeauftragte für den Datenschutz Niedersachsen». La objeción también ha estado coordinada con otras AC de Alemania.
[5] Proyecto de decisión, apartados 1.1-1.2.
[6] Proyecto de decisión, apartado 1.9.
[7] Proyecto de decisión, apartados 2.7 y 4.7.
[8] Proyecto de decisión, apartado 2.10.
[9] Proyecto de decisión, apartado 2.10.
[10] Proyecto de decisión, apartados 1.10, 2.10, 14.2 y 14.3.

5. La decisión adoptada por la AC IE de iniciar la investigación se tomó teniendo en cuenta que TIC, en su formulario de notificación de la violación de la seguridad de los datos, había detectado que el **impacto potencial para las personas afectadas era «significativo»**[11].

6. La AC IE indicó en su Proyecto de decisión que acogía con satisfacción asumir la función de ACP, en el sentido del RGPD, para TIC, en tanto que responsable en relación con el tratamiento transfronterizo de datos personales efectuado por TIC que era objeto de la violación de la seguridad[12].

7. La tabla que figura a continuación presenta una cronología sumaria de los acontecimientos que forman parte del procedimiento que llevó a la presentación del asunto ante el mecanismo de coherencia:

26.12.2018	Twitter, Inc., una sociedad registrada en los Estados Unidos, recibe un informe sobre un defecto de código informático a través de su *bug bounty programme*. El informe fue enviado por un contratista externo que gestionaba el programa (Contratista 1) al contratista externo contratado por Twitter, Inc. para buscar y evaluar los defectos (Contratista 2).
29.12.2018	El Contratista 2 comparte el resultado con Twitter, Inc. a través de un tique JIRA.
02.01.2019	El equipo de seguridad de la información de Twitter, Inc. revisa el tique JIRA y decide que no se trata de una cuestión de seguridad sino que podría tratarse de una cuestión de protección de datos.
02.01.2019	Se informa al equipo jurídico de Twitter, Inc.
03.01.2019	El equipo jurídico de Twitter, Inc. decide que el asunto debe tratarse como un incidente.
04.01.2019	Twitter, Inc. activa el **proceso de respuesta a incidentes**, pero debido a un error en la aplicación del procedimiento interno, no se incluye al delegado de protección de datos (DPD) global como «observador». En consecuencia, el DPD global no recibe ninguna notificación.
07.01.2019	El DPD global recibe información sobre la violación de la seguridad de los datos en el curso de una reunión.
08.01.2019	TIC **notifica la violación** a la AC IE mediante el formulario de notificación de violación de la seguridad de datos transfronterizos de la AC IE.
22.01.2019	El alcance y el fundamento jurídico de la investigación se establecieron en la notificación de inicio de investigación que se envió a TIC el 22 de enero de 2019. La AC IE inicia la investigación y solicita información de TIC.
28.05.2019 a 21.10.2019	Fase de informe de investigación: - la AC IE elabora un **proyecto de informe de investigación** y lo expide a TIC para que TIC pueda presentar alegaciones al respecto;

[11] Proyecto de decisión, apartado 2.8.

[12] La AC IE ha confirmado que su valoración en este sentido se basaba tanto en su determinación de que 1) TIC, como proveedor del servicio de Twitter en la UE/EEE, es el responsable pertinente del tratamiento, y 2) la sede principal de TIC en la UE se encuentra en Dublín, Irlanda, donde TIC toma las decisiones sobre los fines y medios para el tratamiento de los datos personales de los usuarios de Twitter en la UE/EEE, conforme a lo establecido en el artículo 4, apartado 16, del RGPD. Proyecto de decisión, apartados 2.2-2.3.

	J TIC presenta sus alegaciones en relación con el proyecto de informe de investigación; J La AC IE solicita aclaraciones en relación con las alegaciones presentadas por TIC; J La AC IE adopta su informe de investigación final.
21.10.2019	La AC IE inicia la fase de toma de decisiones.
11 y 28.11.2019	La AC IE intercambia correspondencia con TIC e invita a TIC a presentar nuevas alegaciones por escrito.
2.12.2019	TIC presenta nuevas alegaciones a la AC IE en respuesta a la correspondencia de la AC IE de 11 y 28 de noviembre de 2019.
14.03.2020	La AC IE emite un **proyecto de decisión preliminar** (en adelante el «**Proyecto de decisión preliminar**») para TIC, y concluye que TIC infringió el artículo 33, apartados 1 y 5, del RGPD; con ello pretende emitir un apercibimiento conforme al artículo 58, apartado 2, letra b) del RGPD y una multa administrativa conforme al artículo 58, apartado 2, letra i) y el artículo 83, apartado 2, del RGPD.
27.04.2020	TIC presenta a la AC IE sus alegaciones respecto al Proyecto de decisión preliminar.
27.04.2020 - 22.05.2020	La AC IE tiene en cuenta las alegaciones de TIC en relación con el Proyecto de decisión preliminar y elabora su proyecto de decisión para presentarlo a las ACI conforme al artículo 60 del RGPD.
22.05.2020 - 20.06.2020	La AC IE comparte su proyecto de decisión con las ACI conforme al artículo 60, apartado 3, del RGPD. Varias ACI (AC AT, AC DE (representada por la AC DE-Hamburgo), AC DK, AC ES, AC FR, AC HU, AC IT y AC NL) formulan **objeciones** conforme al artículo 60, apartado 4, del RGPD.
15.07.2020	La AC IE emite un memorando colectivo en el que establece sus respuestas a dichas objeciones y lo comparte con las ACI (en lo sucesivo el «**Memorando colectivo**»). La AC IE solicita a las ACI pertinentes que confirmen si, teniendo en cuenta la postura de la AC IE en relación con las objeciones conforme a lo indicado en el Memorando colectivo, las ACI desean mantener sus objeciones.
27 y 28.07.2020	A la luz de los argumentos presentados por la AC IE en el Memorando colectivo, la AC DK informa a la AC IE que retira su objeción, y la AC ES informa a la AC IE que retira su objeción en parte. Las demás ACI (es decir, AT, DE, ES, FR, HU, IT y NL) confirman a la AC IE que mantienen sus objeciones.
19.08.2020	La AC IE remite el asunto al CEPD conforme al artículo 60, apartado 4 del RGPD, iniciando así el procedimiento de resolución de conflictos con arreglo al artículo 65, apartado 1, letra a).

8. La AC IE activó el proceso de resolución de conflictos en el sistema IMI el 19 de agosto de 2020. Tras la remisión del asunto por parte de la ACP al CEPD conforme al artículo 60, apartado 4, del RGPD, la Secretaría del CEPD evaluó la integridad del expediente en nombre de la Presidencia, en consonancia con lo establecido en el artículo 11, apartado 2, del Reglamento interno del CEPD. La Secretaría del CEPD se puso en contacto por primera vez con la AC IE el 20 de agosto de 2020, solicitando documentos e información adicional que debían presentarse en el IMI y solicitando que la AC IE confirmara la integridad del expediente. La AC IE proporcionó los documentos y la información, y confirmó la integridad del expediente el 21 de agosto de 2020. Una cuestión de especial importancia que examinó

la Secretaría del CEPD fue el derecho de toda persona a ser oída, en virtud del artículo 41, apartado 2, letra a) de la Carta de Derechos Fundamentales. El 4 de septiembre de 2020, la Secretaría se puso en contacto con la AC IE y trasladó preguntas adicionales para confirmar si TIC había tenido la oportunidad de ejercer su «derecho a ser oída» en relación con todos los documentos presentados al Comité para tomar una decisión. El 8 de septiembre de 2020, la AC IE confirmó que así era, y presentó los documentos que lo demostraban[13].

9. El 8 de septiembre de 2020, se tomó la decisión relativa a la integridad del expediente, y la Secretaría del CEPD la distribuyó entre todos los miembros del CEPD.

10. De conformidad con el artículo 65, apartado 3 del RGPD y el artículo 11, apartado 4 del Reglamento interno del CEPD, la Presidencia decidió ampliar el plazo por defecto para la adopción de la decisión en un mes adicional, debido a la complejidad del asunto.

2 CONDICIONES PARA LA ADOPCIÓN DE UNA DECISIÓN VINCULANTE

11. Las condiciones generales para la adopción de una decisión vinculante por parte del Comité se establecen en los artículos 60, apartado 4, y 65, apartado 1, letra a) del RGPD[14].

2.1 Objeciones formuladas por las ACI en relación con un proyecto de decisión

12. El CEPD observa que las ACI han formulado objeciones al Proyecto de decisión a través del sistema de información y comunicación mencionado en el artículo 17 del Reglamento interno del CEPD, es decir el Sistema de Información del Mercado Interior. Las objeciones se formularon conforme al artículo 60, apartado 4, del RGPD.

13. Más específicamente, las ACI presentaron objeciones en relación con las cuestiones siguientes:

- la competencia de la ACP;
- La cualificación de las funciones de TIC y Twitter, Inc., respectivamente;
- las infracciones del RGPD identificadas por la ACP;
- la existencia de posibles infracciones adicionales (o alternativas) del RGPD;
- la falta de un apercibimiento;
- el cálculo de la multa propuesta

14. Cada una de esas objeciones se presentó dentro del plazo establecido en el artículo 60, apartado 4, del RGPD.

2.2 La ACP no sigue lo indicado en las objeciones pertinentes y motivadas al proyecto de decisión o es de la opinión que las objeciones no son pertinentes y motivadas

15. El 15 de julio de 2020, la AC IE proporcionó a las ACI un análisis detallado de las objeciones formuladas por las ACI en el Memorando colectivo, donde explicaba si consideraba o no que las objeciones eran

[13] Entre los documentos enviados por la AC IE figuraban mensajes electrónicos del DPD global reconociendo la recepción de los documentos en cuestión.

[14] En virtud del artículo 65, apartado 1, letra a) del RGPD, el Comité emitirá una decisión vinculante cuando una autoridad de control interesada haya manifestado una objeción pertinente y motivada a un proyecto de decisión de la ACP, o esta haya rechazado dicha objeción por no ser pertinente o no estar motivada.

«pertinentes y motivadas» conforme al artículo 4, apartado 24, del RGPD, y si decidía seguir alguna de las objeciones o no[15].

16. Más específicamente, la AC IE consideraba que solo las objeciones formuladas por las ACI en relación con el cálculo de la multa satisfacen lo dispuesto en el artículo 4, apartado 24, del RGPD, en la medida en que se refieren al cumplimiento del RGPD en la actuación prevista en relación con el responsable o el encargado del tratamiento, y describen los riesgos que supone para los derechos y libertades fundamentales de los interesados[16]. Sin embargo, la AC IE decidió que no seguiría lo indicado en las objeciones, por los motivos expuestos en el Memorando colectivo y que se detallan a continuación.

17. La AC IE consideraba que las demás objeciones expresadas por las ACI no eran «pertinentes y motivadas» en el sentido del artículo 4, apartado 24, del RGPD.

2.3 Conclusión

18. El asunto en cuestión cumple todos los elementos mencionados en el artículo 65, apartado 1, letra a), del RGPD, dado que varias ACI formularon objeciones a un proyecto de decisión de la ACP dentro del plazo dispuesto en el artículo 60, apartado 4, del RGPD, y la ACP no ha seguido lo indicado en las objeciones o las ha rechazado por no considerarlas pertinentes y motivadas.

19. El CEPD, por lo tanto, es competente para adoptar una decisión vinculante, que afectará a todas las cuestiones que son objeto de las correspondientes objeciones pertinentes y motivadas, en particular si existe una infracción del RGPD[17].

20. Todos los resultados de esta decisión se entienden sin perjuicio de las evaluaciones o decisiones vinculantes que el CEPD haya tomado en otros asuntos, incluso con las mismas partes, dependiendo de conclusiones adicionales o nuevas.

3 EL DERECHO A UNA BUENA ADMINISTRACIÓN

21. El CEPD está sujeto al artículo 41 de la Carta de los Derechos Fundamentales de la UE, que establece el derecho a una buena administración. Este deber se refleja también en el artículo 11, apartado 1, del Reglamento interno del CEPD[18].

22. La decisión del CEPD «*estará motivada y será dirigida a la autoridad de control principal y a todas las autoridades de control interesadas, y será vinculante para ellas*» (artículo 65, apartado 2, del RGPD). No pretende dirigirse directamente a ninguna tercera parte. No obstante, como medida cautelar para abordar la posibilidad de que TIC pueda verse afectada por la decisión del CEPD, el CEPD valoró si TIC había tenido la oportunidad de ejercer su derecho a ser oída en relación con el procedimiento dirigido por la ACP y, en particular, si todos los documentos recibidos en el procedimiento y utilizados por el

[15] La finalidad del documento, como ha indicado la AC IE, era facilitar una mayor cooperación con las ACI en relación con el Proyecto de decisión y cumplir el requisito establecido enel artículo 60, apartado 1, del RGPD según el cual la ACP debe cooperar con las demás ACI y esforzarse por llegar a un consenso.
[16] Memorando colectivo, apartado 5.59.
[17] Artículo 65, apartado 1, letra a), *in fine*, del RGPD. Algunas ACI han formulado comentarios, que no son objeciones per se, y, por lo tanto, el CEPD no los ha tenido en cuenta.
[18] Reglamento interno del CEPD, aprobado el 25 de mayo de 2018, y su última modificación y adopción del 8 de octubre de 2020.

CEPD para tomar su decisión habían sido compartidos previamente con TIC y si TIC había podido pronunciarse sobre los mismos.

23. Considerando que TIC ya ha sido oída por la AC IE respecto a toda la información recibida por el CEPD y utilizada para tomar su decisión[19], y que la ACP ha compartido con el CEPD las observaciones escritas de TIC, en consonancia con el artículo 11, apartado 2 del Reglamento interno del CEPD[20], en relación con las cuestiones planteadas en este Proyecto de decisión, el CEPD acoge con satisfacción que se haya respetado el artículo 41 de la Carta de los Derechos Fundamentales de la UE.

4 ACERCA DE LA CUALIFICACIÓN DE RESPONSABLE Y ENCARGADO DEL TRATAMIENTO Y LA COMPETENCIA DE LA ACP

4.1 Análisis de la ACP en el Proyecto de decisión

24. En el Proyecto de decisión se indica que «*...al inicio de la Investigación, el investigador designado por la AC IE [...] estuvo de acuerdo en que TIC es el responsable del tratamiento, en el sentido del artículo 4, apartado 7, del RGPD, en relación con los datos personales objeto de la violación de seguridad*», y que «*...en este sentido, TIC confirmó que era el responsable del tratamiento*» en el formulario de notificación de la violación de la seguridad de los datos y en la correspondencia con la AC IE[21]. En el Proyecto de decisión se indica además que «*TIC también confirmó que la violación había surgido en el contexto del tratamiento efectuado en su nombre por Twitter Inc., el encargado del tratamiento*»[22] y que «*TIC es la responsable del tratamiento de los datos personales que son objeto de la investigación. TIC tiene un contrato vigente con Twitter Inc. (su encargado) para prestar servicios de tratamiento de datos*»[23].

25. Asimismo, en el Proyecto de decisión se especifica que la AC IE está convencida de que es competente para actuar como ACP en relación con el tratamiento transfronterizo llevado a cabo por TIC para los datos personales objeto de la violación[24].

26. En este sentido, en el Proyecto de decisión se indica además que, cuando TIC notificó la violación, confirmó a la AC IE que era «*una empresa irlandesa*», y el «*proveedor de los servicios de Twitter en Europa*», y que la Política de Privacidad de TIC (actualizada en enero de 2016) informaba a los usuarios del servicio de Twitter en la UE que tenían derecho a consultar sus dudas tanto a su autoridad de control local como a la ACP de TIC, la AC IE[25].

27. Además, la AC IE incluía en el Proyecto de decisión un extracto del informe anual y los estados financieros de TIC relativos al ejercicio que finalizó el 31 de diciembre de 2018, especificando que «*la parte dominante principal y el grupo más grande de empresas para las que se preparan los estados*

[19] Proyecto de decisión preliminar de la AC IE (14 de marzo de 2020); Proyecto de decisión de la AC IE (22 de mayo de 2020); Objeciones y comentarios planteados por las ACI (18-20 de junio de 2020); Memorando colectivo de la AC IE (15 de julio de 2020); y el resto de comentarios y objeciones de las ACI (27-28 de julio de 2020).
[20] Reglamento interno del CEPD, aprobado el 25 de mayo de 2018, y su última modificación y adopción del 8 de octubre de 2020.
[21] Proyecto de decisión, apartado 2.2.
[22] Proyecto de decisión, apartado 4.2.
[23] Proyecto de decisión, apartado 4.6.
[24] Proyecto de decisión, apartado 2.3.
[25] Proyecto de decisión, apartado 2.3.

financieros del grupo, y del que la empresa es parte, es Twitter, Inc., una sociedad constituida en los Estados Unidos de América y que cotiza en la bolsa de Nueva York»[26].

28. Inicialmente, la AC IE tuvo que resolver las dudas que planteaba el uso de los términos «nosotros» y «nuestro/a» en el formulario de notificación de la violación de la seguridad de los datos respecto a la intercambiabilidad entre TIC y Twitter, Inc. La AC IE pidió una aclaración al respecto y TIC indicó que los empleados de TIC y de Twitter, Inc. suelen utilizar el «nosotros» y el «nuestro/a» de manera general para referirse al grupo por su nombre. Además, TIC indicó que, aunque TIC es el responsable del tratamiento y toma decisiones respecto a los fines y medios del tratamiento de los datos, no opera sola: «*TIC y sus empleados forman parte del [...] Grupo Twitter [...]. Todos los empleados del Grupo Twitter utilizan los mismos sistemas informáticos, siguen las mismas políticas generales... Y trabajan juntos para garantizar la asistencia global las veinticuatro horas necesaria a fin de mantener operativa la plataforma Twitter*»[27].

4.2 Resumen de las objeciones formuladas por las ACI

29. En su objeción, la **AC ES** indica que **el Proyecto de decisión no justifica suficientemente el papel de TIC como responsable del tratamiento**. La AC ES destaca que debería llevarse a cabo una evaluación sobre cuál es la entidad que realmente toma las decisiones en relación con los fines y los medios, además de un análisis crítico de todos los hechos ocurridos. Según la AC ES, los elementos en que se basa el Proyecto de decisión parecen sugerir una conclusión diferente de la alcanzada por la AC IE. En concreto, la AC ES considera que las decisiones sobre los fines esenciales del tratamiento de datos en realidad las toma Twitter, Inc. La AC ES argumenta esta afirmación con una relación de algunos factores que, en su opinión, podrían sugerir que TIC no decide respecto a los fines y medios. En primer lugar, la AC ES recuerda que TIC es una filial de Twitter, Inc. y destaca que, por ese motivo, sería difícil comprender cómo podría TIC «*dar órdenes*» a Twitter, Inc. en relación con el tratamiento de datos personales de usuarios del EEE. Según la AC ES, TIC nunca ha estado en situación de poder elegir independientemente a Twitter, Inc. como su encargado del tratamiento, y tampoco podría elegir a otro. Asimismo, la AC ES argumenta que Twitter, Inc. no parece actuar como encargado del tratamiento debido a la «*ausencia de un canal directo*» entre las dos empresas para la gestión de los asuntos de violación de la seguridad de los datos, aparte de enviar un correo electrónico con el DPD global en copia. En tercer lugar, la AC ES indica que no queda claro cómo podría TIC haber adoptado de forma independiente o influido en las decisiones para corregir el defecto de TI en el sistema gestionado y controlado por Twitter, Inc., y que fue más bien Twitter, Inc. quien tomó las decisiones para resolver la violación, cuyos efectos no se limitaron solo a los usuarios europeos.

30. La **AC NL** también formuló una objeción sobre la cualificación legal de TIC y Twitter, Inc. como responsable y encargado respectivamente. En concreto, la objeción se refiere a la forma como la AC IE ha argumentado que TIC es el único responsable en este asunto, y que Twitter, Inc. es un encargado que actúa en su nombre. La AC NL considera que la evaluación de la responsabilidad es un aspecto fundamental en este asunto y, por lo tanto, toda conclusión relativa a la función del responsable, el encargado o los corresponsables del tratamiento debe demostrarse con evidencia de hecho y de Derecho. En su objeción**, la AC NL afirma esencialmente que el Proyecto de decisión no contiene evidencia suficiente para establecer de forma legal y objetiva las funciones de las entidades en cuestión**, en concreto para justificar la conclusión de que i) TIC es el (único) responsable del tratamiento, y ii) que Twitter, Inc. es un simple encargado que actúa siguiendo instrucciones de TIC para el funcionamiento del servicio de Twitter en todo el mundo y/o los fines que son relevantes en

[26] Proyecto de decisión, apartado 2.4.
[27] Proyecto de decisión, apartado 4.5.

este asunto. Según la AC NL, la ACP debería verificar **si los avisos legales de la organización y/o su política de privacidad corresponden con sus actividades reales**. La AC NL solicita a la AC IE que incluya más información y/o una descripción de los factores en que se basó la determinación de funciones en el propio documento del Proyecto de decisión. La AC NL también menciona, como ejemplos de factores a tener en cuenta, las instrucciones de TIC a Twitter, Inc., u otras pruebas objetivas o indicios prácticos de las operaciones diarias, así como ejemplos de documentación escrita, como el acuerdo sobre el tratamiento de datos.

31. En su objeción, la **AC DE** argumenta que **la relación entre Twitter, Inc. y TIC no es una relación responsable-encargado**, sino más bien una relación de corresponsables. En primera instancia, la objeción se basa en el hecho de que Twitter, Inc. y TIC no gestionan sistemas de tratamiento de datos independientes. Según la AC DE, el sistema básico que gestiona Twitter, Inc. se modifica a partir de decisiones tomadas por TIC para los usuarios del EEE, mientras que el sistema de tratamiento de datos principal sigue siendo el mismo. La AC DE también destaca que todos los empleados del grupo utilizan el mismo sistema informático y siguen las mismas políticas generales.

32. Finalmente, la **AC FR** formuló una objeción sobre la competencia de la AC IE, indicando que daba la impresión de que la AC IE había llegado a la conclusión de que el poder de tomar decisiones sobre los fines y medios del tratamiento en cuestión estaba en manos de TIC. Según la AC FR, **en el Proyecto de decisión no se indica claramente qué otros elementos, aparte de las declaraciones de TIC, se han tenido en cuenta para considerar que esta empresa tenía poder de toma de decisiones sobre el tratamiento**. La AC FR también especifica que el Proyecto de decisión no indica claramente si la competencia de la autoridad se basa en el hecho de que TIC debería considerarse responsable del tratamiento, o porque TIC debería considerarse el establecimiento principal tal como se define en el artículo 4, apartado 16, del RGPD. La AC FR concluye que, en su estado actual, el Proyecto de decisión no impide el riesgo de que se busque un foro de conveniencia, que es lo que se pretende evitar con el mecanismo de ventanilla única. La AC FR invita a la AC IE a proporcionar más elementos que permitan demostrar que la empresa TIC tiene poder de decisión en cuanto a los fines y medios del tratamiento de los datos para la red social Twitter.

4.3 Posición de la ACP respecto a las objeciones

33. En su Memorando colectivo, la AC IE consideraba que una objeción basada en el papel o la designación de las partes como responsable y encargado o en la competencia de la AC IE «*no cuestiona ni el resultado de una infracción ni la actuación prevista y, por lo tanto, no es conforme con la definición del artículo 4, apartado 24*» y que «*no coincide con lo que debe ser una objeción pertinente y motivada con arreglo al artículo 4, apartado 24*»[28]. Sin embargo, la AC IE analizó dichas objeciones y, al hacerlo, estableció los factores que había tenido en cuenta para determinar el papel de TIC como responsable del tratamiento y como establecimiento principal. En este sentido, la AC IE (a modo de resumen[29]) perfila someramente los hechos y el análisis jurídico en el que se basó su conclusión respecto a la posición de TIC como responsable, en esencia:

- la confirmación previa de Twitter en 2015 proponiendo que TIC en Irlanda fuera el responsable del tratamiento de los datos personales de los usuarios de Twitter en la UE[30];

[28] Memorando colectivo, apartado 5.39.
[29] Memorando colectivo, apartado 5.35.
[30] En este sentido, el Memorando colectivo explica que, el 8 de abril de 2015, TIC comunicó a la AC IE que proponía a TIC en Irlanda como responsable del tratamiento de los datos personales de sus usuarios de países

- la confirmación de TIC de que era el responsable de los datos personales afectados por la violación tanto al notificar la violación a la AC IE como en el transcurso de la investigación;
- la confirmación por parte de TIC de que existe un acuerdo sobre el tratamiento de datos entre ella y Twitter, Inc., como su encargado, que incluye las disposiciones requeridas por el artículo 28 del RGPD;
- la interacción entre TIC y Twitter, Inc. posterior al 7 de enero de 2019, cuando (a través de su DPD) TIC fue informada de la violación, lo que, según la AC IE, demuestra que TIC ejercía el control y tenía autoridad por encima de Twitter, Inc. para la toma de decisiones sobre las actividades de reparación y notificación de la violación, y en relación con el tratamiento subyacente de los datos personales afectados por la violación; y
- las acciones de Twitter, Inc. cuando fue informada del incidente por el Contratista 2, lo que, según la AC IE, también demuestra que la relación entre las dos entidades era tal que TIC ejercía autoridad y asumía responsabilidades como responsable del tratamiento.

34. A continuación, la AC IE explica, a modo de resumen[31], los hechos y el análisis jurídico en el que se basó su conclusión de que TIC es el establecimiento principal en Irlanda, en esencia (además de los puntos anteriores):
    - La designación de TIC y su autodeclaración como establecimiento principal;
    - la confirmación en la Política de Privacidad de TIC de su calidad de responsable del tratamiento de los datos personales de los usuarios de Twitter en la UE;
    - la sede de la administración central de TIC se encuentra en Dublín, donde cuenta con aproximadamente 170 empleados;
    - la contratación directa por parte de TIC de un DPD global a efectos del RGPD, la línea jerárquica del DPD global dentro de TIC y la representación de TIC por parte del DPD global en una gama de actividades relacionadas con la privacidad y el tratamiento de datos, incluida la facultad de vetar el tratamiento de datos;
    - la supervisión histórica y continua de TIC por parte de la AC IE durante la cual se ha hecho evidente que TIC decide los fines y los medios del tratamiento de datos personales en la UE.

    La AC IE reitera que, independientemente de su respuesta al contenido de las objeciones formuladas sobre cuestiones de la competencia y/o la designación de las partes, no considera que las objeciones relativas a estas cuestiones sean conformes con la definición de «objeción pertinente y motivada» que establece el artículo 4, apartado 24, del RGPD. La AC IE afirma que, en vista tanto de su evaluación, según la cual estas cuestiones no cumplen la definición del artículo 4, apartado 24 del RGPD, y de su demostración de que ha abordado adecuadamente en el Proyecto de decisión las cuestiones relativas al establecimiento principal, su competencia, y la designación del responsable y el encargado, no tiene intención de seguir lo indicado en las objeciones sobre estos temas[32].

externos a los Estados Unidos, y que TIC notificó este hecho a otras autoridades de control de la UE en mayo de 2015 (apartado 5.15).

[31] Memorando colectivo, apartado 5.36.

[32] Memorando colectivo, apartado 5.40.

4.4 Análisis del CEPD

4.4.1 Evaluación de si las objeciones son pertinentes y motivadas

35. El CEPD iniciará su análisis de las objeciones formuladas valorando si pueden considerarse «objeciones pertinentes y motivadas» en el sentido del artículo 4, artículo 24, del RGPD.

36. El artículo 4, apartado 24, del RGPD define una objeción pertinente y motivada como «*la objeción a una propuesta de decisión sobre la existencia o no de infracción del presente Reglamento, o sobre la conformidad con el presente Reglamento de acciones previstas en relación con el responsable o el encargado del tratamiento, que demuestre claramente la importancia de los riesgos que entraña el proyecto de decisión para los derechos y libertades fundamentales de los interesados y, en su caso, para la libre circulación de datos personales dentro de la Unión*»[33].

37. Según lo establecido en las Directrices sobre el concepto de objeción pertinente y motivada, una objeción tiene que ser a la vez «pertinente» y «motivada». Para que la objeción sea «pertinente», tiene que existir una relación directa entre la objeción y el proyecto de decisión, y tiene que tratar sobre si existe una infracción del RGPD o si la actuación prevista en relación con el responsable o el encargado del tratamiento es conforme al RGPD[34].

38. Según dichas Directrices, una objeción es «motivada» cuando es coherente, clara, precisa y detallada al proporcionar aclaraciones y argumentos sobre por qué se propone una modificación de la decisión y de qué modo el cambio comportaría una conclusión diferente[35], y cuando demuestra claramente la importancia de los riesgos que entraña el proyecto de decisión para los derechos y libertades fundamentales de los interesados y, en su caso, para la libre circulación de datos personales dentro de la Unión Europea. Así pues, las ACI deben «*mostrar las implicaciones que el proyecto de decisión tendría para los valores protegidos*», «*aportando argumentos suficientes para demostrar que dichos riesgos son considerables y plausibles*»[36]. La evaluación de los riesgos planteados para los derechos y libertades de los interesados[37] puede depender, entre otras cosas, de la idoneidad, la necesidad y la proporcionalidad de las medidas propuestas[38] y de la posible reducción de futuras infracciones del RGPD[39].

39. En términos de contenido, como primera alternativa, la objeción puede referirse a la existencia de una infracción del RGPD. En este caso, debe explicar por qué la ACI no está de acuerdo en si las actividades llevadas a cabo por el responsable o el encargado suponen o no una infracción de una determinada

[33] RGPD, artículo 4, apartado 24.
[34] Véanse también el documento de directrices del CEPD sobre las objeciones pertinentes y motivadas *Guidelines 9/2020 on relevant and reasoned objection under Regulation 2016/679* (solo en inglés), versión para consulta pública (en adelante las «**Directrices sobre OPM**»), apartado 12, actualmente sometido a consulta pública, https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-092020-relevant-and-reasoned-objection_en. Las directrices fueron aprobadas el 8 de octubre de 2020 tras el inicio de la investigación por parte de la AC IE respecto a este asunto concreto.
[35] Directrices sobre OPM, apartado 17 y 20.
[36] Directrices sobre OPM, apartado 37.
[37] Los «interesados» cuyos derechos y libertades se ven afectados pueden ser tanto aquellos cuyos datos personales son objeto de tratamiento por el responsable/encargado como aquellos cuyos datos personales puedan ser objeto de tratamiento en el futuro. Directrices sobre OPM, apartado 43.
[38] Directrices sobre OPM, apartado 42.
[39] Directrices sobre OPM, apartado 43.

disposición del RGPD, y qué infracción o infracciones en concreto[40]. Esta objeción también puede incluir un desacuerdo respecto a las conclusiones que se extraen de los resultados de la investigación (p. ej., indicar que los resultados implican una infracción diferente o adicional a las ya analizadas)[41] o incluso puede llegar a identificar defectos en el proyecto de decisión que justifiquen la necesidad de ulterior investigación por parte de la ACP[42]. Sin embargo, es menos probable que esto ocurra si, previamente a la adopción del proyecto de decisión, la ACP ha cumplido la obligación de cooperar con las ACI e intercambiar toda la información relevante[43]. Alternativamente, el contenido de la objeción puede referirse a la conformidad con el RGPD de la actuación relacionada con el responsable o el encargado (medida correctiva o de otro tipo) contemplada en el proyecto de decisión, explicando por qué la actuación prevista no se considera conforme con el RGPD[44].

40. El CEPD considera que es posible que una objeción relativa a la existencia de una infracción del RGPD trate sobre la ausencia o insuficiencia de evaluación o razonamiento (con la consecuencia de que la conclusión del proyecto de decisión no esté adecuadamente fundamentada por la evaluación realizada y la evidencia presentada, como requiere el artículo 58 del RGPD), en la medida en que se cumpla lo dispuesto en el artículo 4, apartado 24, del RGPD y siempre que exista una conexión entre el análisis presuntamente insuficiente y la existencia o no de infracción del RGPD o si la actuación prevista es o no conforme con el RGPD[45].

41. El CEPD considera que una objeción relativa al papel o la designación de las partes puede entrar en el significado de la definición de «objeción pertinente y motivada» conforme al artículo 4, apartado 24, del RGPD, dado que puede afectar a la determinación sobre si existe una infracción del Reglamento o sobre si la actuación prevista en relación con el responsable o el encargado del tratamiento cumple el Reglamento o no. No obstante, el CEPD considera que una objeción respecto a la competencia de la autoridad de control para actuar como ACP no debería plantearse a través de una objeción conforme al artículo 60, apartado 4 del RGPD, y no encaja con el alcance del artículo 4, apartado 24, del RGPD[46].

a) Evaluación de la objeción formulada por la AC NL

42. La objeción formulada por la AC NL en primera instancia se refiere a una «*ausencia o insuficiencia de razonamiento*»[47] para llegar a las conclusiones de la AC IE sobre la calificación legal de TIC y Twitter, Inc. Como indica la AC NL, la evaluación de la responsabilidad es, de hecho, un aspecto fundamental de este asunto. Una decisión diferente en cuanto a la calificación legal de TIC y Twitter, Inc. afectaría

[40] Directrices sobre OPM, apartado 25.
[41] Directrices sobre OPM, apartado 27.
[42] Directrices sobre OPM, apartado 28 (que también especifica que, en este sentido, debe distinguirse entre, por una parte, las investigaciones de iniciativa propia y, por otra parte, las investigaciones iniciadas a partir de reclamaciones o informes sobre posibles infracciones compartidas por las autoridades de control interesadas).
[43] Directrices sobre OPM, apartado 27.
[44] Directrices sobre OPM, apartado 33. Esto significa que la objeción puede cuestionar, entre otras cosas, los elementos en los que se basa el cálculo del importe de la multa (Directrices sobre OPM, apartado 34).
[45] Directrices sobre OPM, apartado 29.
[46] En este caso es aplicable el procedimiento descrito en el artículo 65, apartado 1, letra b) del RGPD y se puede iniciar en cualquier fase según las Directrices sobre OPM, apartado 31.
[47] Directrices sobre OPM, apartado 29. Una objeción pertinente y motivada en relación con si existe una infracción del RGPD puede referirse a «*falta de información sobre los hechos o de una descripción del asunto en cuestión», o a un «desacuerdo en cuanto a las conclusiones que deben extraerse de los resultados de la investigación*» (Directrices sobre OPM, apartado 27) o referirse a una «*ausencia o insuficiencia de evaluación o razonamiento (con la consecuencia de que la conclusión del proyecto de decisión no esté bien argumentada con la evaluación efectuada y la evidencia presentada, según requiere el artículo 58 del RGPD)*» (Directrices sobre OPM, apartado 29).

a las conclusiones de la autoridad de control, tanto en relación con la determinación de una infracción del artículo 33 del RGPD, como en relación con las medidas correctivas resultantes de la investigación.

43. El CEPD recuerda que toda medida jurídicamente vinculante de una autoridad de control debe especificar los motivos de la medida[48]. La decisión sobre si existe una infracción del Reglamento, o sobre si la actuación prevista en relación con el responsable o el encargado es conforme con el Reglamento, depende de la identificación correcta de las funciones de las partes que serán objeto de la medida en cuestión. Por lo tanto, un proyecto de decisión debe contener elementos de hecho y de Derecho suficientes para respaldar la decisión propuesta[49]. Como resultado, el CEPD considera que la objeción formulada por la AC NL se refiere tanto a «si existe una infracción del RGPD» como a «si la acción prevista es conforme o no con el RGPD».

44. Aunque el CEPD considera que la objeción de la AC NL es pertinente e incluye argumentos jurídicos que respaldan su postura, no argumenta detalladamente de qué manera dichas consecuencias entrañan un riesgo significativo para los derechos y libertades de los interesados y/o la libre circulación de datos[50]. El CEPD recuerda que la obligación de demostrar claramente la importancia del riesgo que entraña el proyecto de decisión, como establece el RGPD, recae en la ACI[51]. A pesar de que la posibilidad de que las ACI puedan proporcionar dicha evidencia también puede depender del grado de detalle del propio proyecto de decisión, y de los intercambios previos de información[52], dicha circunstancia, en caso de ser aplicable, no puede eximir por completo a la ACI de la obligación de explicar con claridad por qué considera que el proyecto de decisión, si no se modifica, entraña un riesgo considerable para los derechos y libertades de los interesados.

45. El CEPD considera que la objeción formulada por la AC NL no demuestra claramente los riesgos para los derechos y libertades de los individuos como tales. En este sentido, el CEPD considera que la objeción formulada por la AC NL no cumple los requisitos del artículo 4, apartado 24, del RGPD.

b) Evaluación de la objeción formulada por la AC ES

46. La objeción formulada por la AC ES también cuestiona la suficiencia de la evaluación o el razonamiento en relación con las conclusiones extraídas por la AC IE en cuanto a la calificación jurídica de TIC y Twitter, Inc. respectivamente. La objeción también deja claro que la calificación correcta de TIC y Twitter, Inc. es esencial para determinar sus respectivas responsabilidades, así como para la competencia de la AC IE. Como resultado, el CEPD también considera que la objeción formulada por la AC ES se refiere tanto a «si existe una infracción del RGPD» como a «si la actuación prevista es conforme o no con el RGPD». La objeción de la AC ES también establece por qué considera que es necesario cambiar el Proyecto de decisión y de qué forma el cambio comportaría una conclusión diferente.

47. Aunque el CEPD considera que la objeción de la AC ES es pertinente e incluye argumentos jurídicos que respaldan esta decisión, no articula claramente por qué esta decisión, si se deja tal cual en este sentido, entrañaría un riesgo significativo para los derechos y libertades de los interesados y/o la libre

[48] Considerando 129 del RGPD.
[49] Dicha información también es necesaria para garantizar la eficiencia de la cooperación y del mecanismo de coherencia, de modo que las ACI puedan tomar una decisión informada sobre si están de acuerdo o no o para expresar una objeción pertinente y motivada.
[50] Directrices sobre OPM, apartado 19.
[51] Directrices sobre OPM, apartado 36 y artículo 4, apartado 24, del RGPD.
[52] Directrices sobre OPM, apartado 36.

circulación de datos. En este sentido, el CEPD considera que la objeción formulada por la AC ES no cumple los requisitos del artículo 4, apartado 24, del RGPD.

c) Evaluación de la objeción formulada por la AC DE

48. Mientras que las objeciones expresadas por la AC NL y la AC ES se refieren principalmente a la «ausencia de razonamiento» que justifique la conclusión de que TIC actúa como responsable (exclusivo), la AC DE no está de acuerdo con las conclusiones que se derivan de los resultados de la investigación[53]. En concreto, la AC DE considera que los elementos de hecho incluidos en el expediente son suficientes para justificar la conclusión de que Twitter, Inc. no es el encargado, sino un corresponsable, junto con TIC.

49. En su objeción, la AC DE también especifica por qué la calificación de las partes es relevante para la determinación de «si existe infracción o no». En concreto, la AC DE argumenta que la evaluación jurídica de la relación entre Twitter, Inc. y TIC afecta a la determinación del momento en que tuvieron constancia de la violación de la seguridad. Según la AC DE, a la luz del artículo 26, apartado 1, del RGPD, el conocimiento debe atribuirse a partes iguales a todos los (cor)responsables. Teniendo esto en cuenta , la AC DE argumenta que la AC IE debe reconsiderar la fecha en la que TIC como corresponsable tuvo conocimiento (o debería haber tenido conocimiento) de la violación.

50. El CEPD considera que la objeción formulada por la AC DE establece claramente por qué se considera necesario cambiar el Proyecto de decisión y cómo la objeción, en caso de seguirse, comportaría una conclusión diferente. Dicho esto, el CEPD no considera que la objeción formulada por la AC DE incluya una afirmación clara sobre los riesgos que entraña el Proyecto de decisión para los derechos y libertades fundamentales de los interesados en relación con la calificación de las partes como tales. En este sentido, el CEPD considera que la objeción formulada por la AC DE no cumple los requisitos del artículo 4, apartado 24, del RGPD.

d) Evaluación de la objeción formulada por la AC FR

51. En esencia, la AC FR considera también que el Proyecto de decisión adolece de «ausencia o insuficiencia de evaluación o razonamiento» porque no indica claramente qué otros elementos, aparte de las propias declaraciones de TIC, tuvo en cuenta la AC IE para considerar que TIC ejerció la facultad de toma de decisiones sobre el tratamiento. Al igual que la AC NL y la AC ES, la AC FR también destaca la importancia de que la decisión de la ACP no esté suficientemente razonada. Pero, al contrario que la AC NL y la AC ES, la AC FR en su objeción se centra principalmente en la importancia de incluir dicho razonamiento al establecer la competencia de una autoridad de la ACP, en particular de cara a impedir que se elija un foro de conveniencia.

52. El CEPD recuerda que un desacuerdo respecto a la competencia de la autoridad de control para emitir una decisión en calidad de ACP no debería plantearse a través de una objeción conforme al artículo 60, apartado 4, del RGPD, y no entra en el alcance del artículo 4, apartado 24, del RGPD[54]. El CEPD considera que la objeción formulada por la AC FR no aporta argumentos suficientes para demostrar claramente la importancia del riesgo que el Proyecto de decisión entraña para los derechos y libertades de los interesados. Por lo tanto, el CEPD considera que la objeción formulada por la AC FR no constituye una objeción pertinente y motivada en el sentido del artículo 4, apartado 24, del RGPD.

[53] Directrices sobre OPM, apartado 27.

[54] Directrices sobre OPM, apartado 31. En las Directrices se establece que, al contrario de la objeción conforme al artículo 60, apartado 4, del RGPD, el procedimiento derivado del artículo 65, apartado 1, letra b), del RGPD se puede aplicar en cualquier momento.

4.4.2 Conclusión

53. El CEPD considera que las objeciones mencionadas cumplen varios criterios del artículo 4, apartado 24, del RGPD. Al contrario que la conclusión expresada por la AC IE, el CEPD considera que cada una de esas objeciones cumple la condición de referirse alternativamente a si existe una infracción de dicho Reglamento o si la actuación prevista en relación con el responsable o el encargado cumple el Reglamento. Asimismo, el CEPD considera que una objeción basada en el papel, o la designación, de las partes, en principio, podría encajar dentro del significado de la definición de «objeción pertinente y motivada» del artículo 4, apartado 24, del RGPD.

54. Pero, como ya se ha dicho, las objeciones mencionadas no cumplen el requisito de proporcionar una demostración clara de la importancia de los riesgos que entraña el Proyecto d decisión en cuanto a los derechos y libertades fundamentales de los interesados y, si procede, la libre circulación de datos personales en la Unión Europea.

55. Asimismo, en lo que se refiere a la objeción presentada por la AC FR, además de no aportar argumentos suficientes para demostrar claramente la importancia del riesgo que entraña el Proyecto de decisión para los derechos y libertades de los interesados, la objeción se refiere al desacuerdo respecto a la competencia de la autoridad de control que actúa en calidad de ACP. El CEPD recuerda que dicho desacuerdo no debería plantearse a través de una objeción conforme al artículo 60, apartado 4, del RGPD, y no está incluida dentro del alcance del artículo 4, apartado 24, del RGPD[55].

56. En este sentido, el CEPD considera que las objeciones formuladas no satisfacen los requisitos del artículo 4, apartado 24, del RGPD.

57. En consecuencia, **el CEPD no se pronuncia sobre el fondo de ninguna cuestión sustancial planteada en dichas objeciones**. **El CEPD reitera que su decisión actual se entiende sin perjuicio de posibles evaluaciones que se puedan requerir del CEPD en otros asuntos, incluso con las mismas partes, teniendo en cuenta el contenido del Proyecto de decisión en cuestión y las objeciones formuladas por las ACI**.

5 ACERCA DE LAS INFRACCIONES DEL RGPD IDENTIFICADAS POR LA ACP

5.1 Sobre los resultados relativos a una infracción del artículo 33, apartado 1, del RGPD

5.1.1 Análisis de la ACP en el Proyecto de decisión

58. La AC IE llegó a la conclusión de que TIC no cumplió sus obligaciones como responsable del tratamiento conforme al artículo 33, apartado 1, del RGPD, que, «*no se puede valorar por sí sola y debe entenderse en el contexto de las obligaciones más amplias de los responsables en virtud del RGPD, en particular la obligación de responsabilidad proactiva conforme al artículo 5, apartado 2, la relación entre*

[55] Directrices sobre OPM, apartado 31.

responsables y encargados del tratamiento (artículo 28) y la obligación de implementar medidas técnicas y organizativas adecuadas (y efectivas)»[56].

59. En relación con el momento en que el responsable tuvo constancia de la violación de la seguridad, el Proyecto de decisión concluye que, en el caso de que la violación la haya sufrido el encargado, el responsable tiene conocimiento de la misma cuando el encargado la notifica[57], pero el responsable debe asegurarse de que ha implantado medidas suficientes para facilitar este conocimiento[58]. Dado que TIC como responsable del tratamiento tenía también la responsabilidad de supervisar las operaciones de tratamiento llevadas a cabo por su encargado Twitter, Inc.[59], el Proyecto de decisión proclama que, si el encargado no sigue el procedimiento o el procedimiento falla, el responsable no puede justificar el hecho de no haber tenido conocimiento del fallo culpando al encargado[60], porque el desempeño de un responsable de su obligación de notificar no puede depender de si el encargado cumple o no sus obligaciones conforme al artículo 33, apartado 2 del RGPD[61]. La AC IE consideró que en esas circunstancias debía tenerse en cuenta que el responsable debía tener un conocimiento constructivo de la violación de los datos personales a través de su encargado[62], y que dicha interpretación refleja la responsabilidad pasiva y proactiva del responsable en el RGPD[63].

60. Así pues, según el Proyecto de decisión, TIC tuvo constancia de la violación de la seguridad el 7 de enero de 2019[64] pero debería haber tenido conocimiento de ella como muy tarde el 3 de enero de 2019, dado que, en dicha fecha, Twitter, Inc., en su calidad de encargado, valoró el incidente por primera vez como una posible violación de la seguridad de los datos, y el equipo jurídico de Twitter, Inc. dio instrucciones de que se abriera un expediente[65]. El Proyecto de decisión indica también que incluso en las circunstancias especiales de esta situación (en la que también hubo retrasos

[56] Proyecto de decisión, apartado 6.20. Véase también Proyecto de decisión, apartados 6.5, 6.7, y 6.13. En el Proyecto de decisión (apartado 7.129 (i)) también se establece que «*el requisito del artículo 33, apartado 1 [...] se basa en el hecho de que el responsable debe garantizar que cuenta con procedimientos y sistemas internos (y, si procede, procedimientos y sistemas implantados en todas las partes externas, incluidos los encargados) configurados y seguidos de forma que faciliten un conocimiento inmediato y una notificación puntual de las violaciones de la seguridad*».

[57] Proyecto de decisión, apartado 7.129 (iii).

[58] Proyecto de decisión, apartado 7.98.

[59] Proyecto de decisión, apartado 7.129 (iv).

[60] Proyecto de decisión, apartado 7.129 (iv).

[61] Proyecto de decisión, apartado 7.129 (x).

[62] Proyecto de decisión, apartado 7.129 (v).

[63] Proyecto de decisión, apartado 7.98. Así pues, con arreglo al Proyecto de decisión, una interpretación alternativa según la cual un responsable solo «tiene constancia» cuando es informado por el encargado, deja una laguna significativa en la protección que ofrece el RGPD, porque podría comportar que el responsable evitara sus responsabilidades, incluso en casos de retrasos importantes, si se demostrara que ha cumplido con sus obligaciones al elegir al encargado y tener implantados los sistemas adecuados, pero dichos sistemas han sido ignorados por el encargado (Proyecto de decisión, apartado 7.99). La AC IE explica, además, en el Proyecto de decisión que la aplicación alternativa del artículo 33, apartado 1, que fue sugerida por TIC, según la cual el cumplimiento de la obligación del responsable de notificar depende, esencialmente, del cumplimiento por parte de su encargado de su obligación de notificar conforme al artículo 33, apartado 2, socavaría la eficacia de las obligaciones del artículo 33 respecto al responsable [y que] dicho punto de vista es contradictorio con la finalidad general del RGPD y la intención del legislador de la UE».

[64] Proyecto de decisión, apartado 7.129 (vi).

[65] Proyecto de decisión, apartado 7.129 (vi).

anteriores[66]), los acuerdos vigentes con Twitter, Inc. lo habrían permitido[67]. En cambio, «debido a la ineficiencia del proceso» en las «circunstancias específicas» del asunto en cuestión y/o «a un fallo del personal [del encargado] a la hora de seguir su proceso de gestión de incidentes», hubo un retraso que hizo que el responsable no fuera notificado hasta el 7 de enero de 2019[68]. Esta fue la causa de la infracción del artículo 33, apartado 1, del RGPD, incluso aunque hubieran transcurrido menos de 72 horas entre el momento en que TIC tuvo constancia de la violación de la seguridad (7 de enero de 2019) y la notificación (8 de enero de 2019).

5.1.2 Resumen de las objeciones formuladas por las ACI

61. La **AC FR** formuló una objeción indicando que los resultados no se corresponden con una infracción del artículo 33, apartado 1, del RGPD, sino más bien con el artículo 28 o el artículo 32 del RGPD, que establecen las obligaciones del responsable cuando decide recurrir a un encargado. Este argumento se deriva del hecho de que el resultado de infracción del artículo 33, apartado 1 se basa principalmente en los fallos ocurridos en la aplicación del procedimiento establecido entre TIC y su encargado en caso de violación de la seguridad de los datos, mientras que el artículo 33, apartado 1, del RGPD se refiere solo a la obligación del responsable de notificar las violaciones de la seguridad a la autoridad competente.

62. Las objeciones de la **AC DE**, en cambio, se centran en el argumento que permite concluir que se infringió el artículo 33, apartado 1, de RGPD, sin cuestionar esta conclusión per se, y se refieren más específicamente a la determinación de cuándo empieza el plazo de 72 horas (*dies a quo*).

63. La AC DE argumenta en su objeción que la cuestión de la asignación de funciones influye en la determinación del momento en que se tuvo conocimiento de la violación, dado que dicho conocimiento se inicia en el mismo momento para los corresponsables del tratamiento. Según la AC DE esto puede llevar a considerar el 26 de diciembre de 2018 como la fecha en la que TIC como corresponsable tuvo o debería haber tenido conocimiento de la violación de la seguridad.

5.1.3 Posición de la ACP respecto a las objeciones

64. En cuanto a la objeción planteada por la AC FR, la AC IE opina que requiere la consideración de otras disposiciones del RGPD, y que la solicitud de las ACI de tener en cuenta disposiciones alternativas del RGPD implicaría esencialmente repensar toda la investigación realizada[69]: la AC IE llegó a la conclusión de que dicha objeción no entra en la definición de «objeción pertinente y motivada» a efectos del artículo 4, apartado 24, del RGPD[70]. La AC IE también destaca su opinión de que hubo una infracción del artículo 33, apartado 1, del RGPD, y no tiene intención de considerar infracciones de otras disposiciones del RGPD como alternativa al artículo 33, apartado 1[71], subrayando que, si ampliara la gama de infracciones a otras obligaciones del RGPD a petición de las ACI, «*perjudicaría la totalidad de*

[66] Al identificar el 3 de enero de 2019 como la fecha en que TIC debería haber tenido conocimiento de la violación de la seguridad, la AC IE también tuvo en cuenta que había habido un retraso anterior durante el período transcurrido entre el momento en que el incidente fue notificado por el contratista externo (Contratista 2) a Twitter, Inc., el 29 de diciembre de 2018, y el momento en que Twitter, Inc. inició su revisión del mismo, el 2 de enero de 2019. En el transcurso de la investigación, TIC confirmó que «*fue debido al calendario de fiestas de invierno*».
[67] Proyecto de decisión, apartado 7.129 (ix).
[68] Proyecto de decisión, apartado 7.129 (vi).
[69] Memorando colectivo, apartado 5.45.
[70] Memorando colectivo, apartado 5.45.
[71] Memorando colectivo, apartado 5.47.

la investigación y el proceso del artículo 60 al exponerlo al riesgo de reclamaciones por falta de equidad procesal»[72]. La AC IE también indica que está examinando el cumplimiento de TIC con sus obligaciones más amplias en virtud del RGPD en el contexto de otra investigación en curso[73].

65. En lo que se refiere a la objeción formulada por la AC DE, que trata específicamente de la determinación del momento en que se tuvo conocimiento de la violación de la seguridad, la AC IE responde que incluso aunque existiera una relación de corresponsabilidad (opinión que, como se ha dicho en el apartado 4.3, la AC IE no comparte) ello no significaría necesariamente que el conocimiento de la violación tuviera que atribuirse equitativamente a ambos corresponsables del tratamiento[74].

5.1.4 Análisis del CEPD

5.1.4.1 Evaluación de si las objeciones son pertinentes y motivadas

66. Como se ha recordado anteriormente (ver apartado 4.4.1), es necesario evaluar si las objeciones formuladas por las ACI son conformes a lo establecido en el artículo 4, apartado 24, del RGPD.

67. Aunque la objeción de la **AC FR** es pertinente, dado que muestra su desacuerdo sobre si ha habido una infracción particular del RGPD en este asunto específico, e incluye argumentos jurídicos para respaldar la objeción, no cumple el artículo 4, apartado 24, del RGPD, porque no incluye ninguna justificación sobre las consecuencias de emitir una decisión sin los cambios propuestos en la objeción, y de qué manera dichas consecuencias entrañarían un riesgo significativo para los derechos y libertades de los interesados[75]. Así pues, no se puede decir que la objeción «demuestre claramente» la importancia de los riesgos que entraña la adopción del Proyecto de decisión (si se publicara definitivamente sin cambios) dado que no aporta argumentos suficientes sobre por qué los derechos y libertades de los interesados en relación con la infracción del artículo 33, apartado 1 (en vez del artículo 32, apartado 28) del RGPD son sustanciales y plausibles[76]. Por lo tanto, el CEPD concluye que la objeción de la **AC FR** no es pertinente y motivada debido a la falta de una demostración clara de los riesgos, concretamente en relación con el artículo 4, apartado 24, del RGPD.

68. Asimismo, en relación con la objeción de la **AC DE**, específicamente sobre el hecho de que la determinación del inicio (*dies a quo*) de la infracción del artículo 33, apartado 1, del RGPD depende de la calificación de las partes, el CEPD quiere recordar el análisis realizado más arriba en el apartado 4.4 y considera que la objeción no demuestra las implicaciones que tendría el Proyecto de decisión con su contenido actual —específicamente sobre el razonamiento respecto a la infracción del artículo 33, apartado 1 del RGPD— para los valores protegidos[77] (derechos y libertades de los interesados, libre circulación de datos personales).

5.1.4.2 Conclusión

69. El CEPD considera que las objeciones mencionadas satisfacen la condición de referirse o bien a si existe una infracción del RGPD o bien a si la actuación prevista en relación con el responsable o el encargado del tratamiento cumple el Reglamento, pero no demuestra claramente la importancia de los riesgos

[72] Memorando colectivo, apartado 5.44 (c).
[73] Memorando colectivo, apartado 5.44 (d).
[74] Memorando colectivo, apartado 5.34 (que se refiere también a la sentencia del TJUE en *Wirtschaftsakademie*, C-210/16, apartado 43).
[75] Directrices sobre OPM, apartado 19.
[76] Directrices sobre OPM, apartado 37.
[77] Directrices sobre OPM, apartado 37.

que el Proyecto de decisión entraña para los derechos y libertades fundamentales de los interesados y, en su caso, para la libre circulación de datos personales dentro de la Unión.

70. Por lo tanto, las objeciones de las AC FR y DE no satisfacen los requisitos del artículo 4, apartado 24 del RGPD[78].

5.2 Sobre los resultados relativos a una infracción del artículo 33, apartado 5, del RGPD

5.2.1 Análisis de la ACP en el Proyecto de decisión

71. En el Proyecto de decisión, la AC IE indicaba que TIC no había cumplido sus obligaciones de documentar la violación conforme al artículo 33, apartado 5, del RGPD, porque consideraba que la documentación presentada por TIC en el transcurso de la investigación no contenía suficiente información y no incluía un registro o documentaba específicamente una «violación de la seguridad de los datos personales», dado que se trataba solo de «documentación de naturaleza más general»[79].

72. Por otro lado, en cambio, la AC IE reconocía que TIC había cooperado plenamente durante la investigación (aunque esto no se consideró un factor atenuante)[80].

5.2.2 Resumen de las objeciones formuladas por las ACI

73. El CEPD aprovecha la oportunidad de destacar, a efectos de una mayor claridad, que ninguna de las objeciones formuladas cuestionaba la conclusión de que TIC había infringido el artículo 33, apartado 5, del RGPD.

74. Sin embargo, la **AC IT** formuló una objeción argumentando que el resultado relativo a la infracción del artículo 33, apartado 5, del RGPD no parece coherente con el razonamiento y las elaboraciones presentadas por la ACP, dado que la inadecuación de la documentación que se presentó durante una investigación tan exhaustiva a partir de las múltiples interacciones entre la ACP y el responsable del tratamiento, presuntamente indica una falta de colaboración del responsable con la APD. Según la AC IT, la conclusión del Proyecto de decisión de que TIC había colaborado plenamente durante la fase de investigación debería revisarse, dado que solo se puede considerar que ha habido una plena colaboración si el responsable ha presentado sin trabas una documentación adecuada y exhaustiva.

5.2.3 Posición de la ACP respecto a las objeciones

75. La AC IE opina que la obligación del artículo 33, apartado 5, del RGPD se aplica independientemente de la obligación derivada del artículo 31 del RGPD de cooperar con la autoridad de control y de cómo se haya comportado TIC al respecto y de cómo haya interactuado con la ACP en el momento en que esta última haya iniciado sus actividades reguladoras respecto a la violación de la seguridad por parte de TIC[81]. La AC IE argumenta que las deficiencias de cómo TIC documentó la violación de la seguridad

[78] En consecuencia, el CEPD no se pronuncia sobre el fondo de ninguna cuestión sustancial planteada en dichas objeciones. El CEPD reitera que su decisión actual ese entiende sin perjuicio de posibles evaluaciones que se puedan requerir del CEPD en otros asuntos, incluso con las mismas partes, teniendo en cuenta el contenido del Proyecto de decisión en cuestión y las objeciones formuladas por las ACI.
[79] Proyecto de decisión, apartado 10.46.
[80] Proyecto de decisión, apartado 14.50.
[81] Memorando colectivo, apartado 5.87.

no implican necesariamente una falta de cooperación por parte de TIC[82]. Además, la AC IE destaca que TIC cooperó con la AC IE durante la investigación respondiendo a todas las peticiones de información y proporcionando todos los documentos solicitados, sin intentar obstruir la investigación de ningún modo[83]. En cualquier caso, la AC IE no consideró que la cooperación de TIC fuera un factor atenuante[84]. Por los motivos mencionados, la AC IE considera que es «cuestionable» que la objeción formulada por la AC IT sea motivada y pertinente, porque, aunque se refiere a una infracción del RGPD, no demuestra que la postura de la AC IE respecto al grado de cooperación de TIC comporte que el Proyecto de decisión entrañe un riesgo para los derechos y libertades fundamentales de los interesados[85]. La AC IE concluyó que no seguiría lo indicado en dicha objeción[86].

5.2.4 Análisis del CEPD

5.2.4.1 Evaluación de si las objeciones son pertinentes y motivadas

76. La AC IT en su objeción no discute que ha habido una infracción del artículo 33, apartado 5, del RGPD. Una objeción pertinente y motivada puede cuestionar el razonamiento de las conclusiones a que ha llegado la ACP en el proyecto de decisión pero solo en la medida en que dicho razonamiento esté relacionado con dichas conclusiones, la objeción estará debidamente motivada. En este asunto, la objeción no argumenta claramente cómo el hecho de seguirla implicaría un cambio en el Proyecto de decisión. Además, la objeción no cumple los criterios indicados en el artículo 4, apartado 24, del RGPD, porque no demuestra claramente la importancia de los riesgos que entraña el Proyecto de decisión, dado que no muestra las implicaciones que el presunto error en el Proyecto de decisión tendría para los valores protegidos.

5.2.4.2 Conclusión

77. Dado que la objeción de la AC IT no cumple los requisitos del artículo 4, apartado 24, del RGPD, el Comité no se pronuncia sobre el fondo de ninguna cuestión sustancial en dicha objeción. El CEPD reitera que su decisión actual se entiende sin perjuicio de posibles evaluaciones que se puedan requerir del CEPD en otros asuntos, incluso con las mismas partes, teniendo en cuenta el contenido del Proyecto de decisión en cuestión y las objeciones formuladas por las ACI.

6 SOBRE POSIBLES INFRACCIONES ADICIONALES (O ALTERNATIVAS) DEL RGPD IDENTIFICADAS POR LAS ACI

6.1 Análisis de la ACP en el Proyecto de decisión

78. A partir de la información proporcionada por TIC cuando notificó la violación de seguridad a la AC IE, la AC IE observó que según el formulario de notificación era evidente que había transcurrido un período de más de 72 horas desde el momento en que TIC (como responsable del tratamiento) tuvo conocimiento de la violación[87]. Por este motivo, la AC IE decidió poner en marcha, por iniciativa propia,

[82] Memorando colectivo, apartado 5.87.
[83] Memorando colectivo, apartado 5.87.
[84] Memorando colectivo, apartado 5.87.
[85] Memorando colectivo, apartado 5.88.
[86] Memorando colectivo, apartado 5.88.
[87] Proyecto de decisión, apartado 2.11.

una investigación para examinar si TIC había cumplido sus obligaciones conforme al artículo 33, apartado 1 y el artículo 33, apartado 5, del RGPD[88].

79. Para determinar si TIC cumple sus obligaciones conforme al artículo 33, apartado 1, del RGPD, la AC IE las ha considerado en el contexto de unas obligaciones más amplias como responsable del tratamiento, incluidas las de la responsabilidad proactiva (artículo 5, apartado 2, del RGPD), las de elección de un encargado (artículo 28 del RGPD), y en relación con la seguridad del tratamiento de los datos personales (artículo 32, del RGPD)[89]. Sin embargo, si bien la AC IE ha tenido en cuenta los factores y las cuestiones de hecho que provocaron el retraso en la notificación de la violación a TIC por parte del encargado, y, en definitiva, el retraso en la notificación de la violación a la AC IE, la AC IE no ha tenido en cuenta si TIC cumplió o no todas o cada una de dichas obligaciones excepto para la finalidad de evaluar el cumplimiento de TIC de sus obligaciones conforme al artículo 33, apartados 1 y 5, del RGPD[90].

6.2 Resumen de las objeciones formuladas por las ACI

80. Las AC DE, FR, HU e IT formularon objeciones sobre otras infracciones de las disposiciones del RGPD por parte de TIC además de o en vez de las del artículo 33, apartados 1 y 5, del RGPD.

6.2.1 Infracción del artículo 5, apartado 1, letra f), del RGPD sobre el principio de integridad y confidencialidad

81. La **AC DE** formuló una objeción en la que indicaba que el «defecto de código subyacente» en la aplicación de TIC que provocó la violación de la seguridad notificada a la AC IE tendría que haber sido tratado por la AC IE en su Proyecto de decisión, con el fin de determinar si este defecto constituyó realmente una violación significativa de la confidencialidad de los datos personales, con una infracción del artículo 5, apartado 1, letra f), del RGPD, además del artículo 33, apartados 1 y 5, del RGPD.

82. La **AC HU** formuló una objeción indicando que, dado el «defecto» en la aplicación de TIC a lo largo de los años y la gravedad de su naturaleza al afectar a la seguridad de los datos, la AC IE debería investigar si TIC también infringió el artículo 5, apartado 1, letra f), del RGPD sobre el principio de integridad y confidencialidad.

6.2.2 Infracción del artículo 5, apartado 2, del RGPD sobre el principio de responsabilidad proactiva

83. La **AC IT** formuló una objeción indicando que la infracción del artículo 33, apartado 1, del RGPD pone de relieve una infracción mucho más grave de la responsabilidad proactiva (con arreglo al artículo 5, apartado 2, del RGPD), dado que la falta de políticas corporativas para gestionar incidentes de seguridad, o el hecho de no cumplirlas, demuestra que las medidas implementadas por el responsable son inadecuadas para garantizar el cumplimiento y documentarlo. La AC IT argumenta que estas deficiencias del procedimiento se mencionan en el Proyecto de decisión, pero no son objeto de un análisis específico. Dado que esto puede afectar también a la gestión de futuras violaciones de la seguridad de los datos, en opinión de la AC IT, las conclusiones sobre si TIC cumplió el artículo 5, apartado 2, del RGPD también deberían ser parte de la decisión final de la AC IE. La AC IT también considera que la infracción del artículo 5, apartado 2, del RGPD queda confirmada por la incapacidad

[88] Proyecto de decisión, apartado 2.11.
[89] Proyecto de decisión, apartados 6.13 a 6.20, 7.111-7.112, 7.122 a 7.124.
[90] Proyecto de decisión, apartados 6.13, 7.111, 7.122 a 7.124.

del responsable de indicar el número exacto y la naturaleza de los datos personales afectados, o el número total de interesados implicados.

6.2.3 Infracción del artículo 24 del RGPD sobre la responsabilidad del responsable del tratamiento

84. La **AC DE** formuló una objeción indicando que el Proyecto de decisión no establece claramente por qué la AC IE no evaluó si la grave violación de la confidencialidad de los datos personales ocasionada por un «defecto subyacente» se debe a una infracción de los requisitos del artículo 24 del RGPD.

6.2.4 Infracción del artículo 28 del RGPD sobre la relación con los encargados del tratamiento

85. La **AC FR** expresó una objeción indicando que TIC no respetó la obligación del responsable de verificar la validez de los procedimientos establecidos por su encargado del tratamiento. Por lo tanto, la AC FR considera que no existe una infracción del artículo 33, apartado 1, del RGPD sino del artículo 28 del RGPD (o el artículo 32 del RGPD, véase el apartado siguiente 6.2.5). La AC FR argumenta que si el encargado del tratamiento de TIC es su empresa matriz, «*era mucho más fácil para TIC verificar la validez de los procedimientos establecidos por la empresa matriz y exigir una corrección si era necesario*».

86. La **AC IT** expresó una objeción indicando que el hecho de que TIC no haya implicado al DPD global en el equipo de detección y respuesta del encargado del tratamiento (Twitter, Inc.), a pesar de que esta práctica se prevé en las políticas internas de TIC, demuestra que las garantías proporcionadas por el encargado del tratamiento para aplicar medidas técnicas y organizativas apropiadas conforme al artículo 28, apartado 1, del RGPD no son suficientemente amplias. Además, la AC IT argumenta en sus objeciones que el encargado incumplió su obligación de ayudar al responsable conforme al artículo 28, apartado 3, letra f), del RGPD.

6.2.5 Infracción del artículo 32 del RGPD sobre la seguridad del tratamiento

87. La **AC DE** formuló objeciones indicando que la AC IE debería haber examinado si en este asunto se cumplieron todas las medidas técnicas y organizativas adecuadas (conforme al artículo 32, del RGPD) y si las infracciones en este aspecto deberían haber sido objeto del presente procedimiento. La AC DE también argumenta que el Proyecto de decisión no establece claramente por qué la AC IE no evaluó si la grave violación de la confidencialidad de los datos personales ocasionada por un «defecto subyacente» se debe a una infracción de los requisitos contemplados en el artículo 32 del RGPD.

88. La **AC FR** expresó una objeción sobre la caracterización jurídica de los hechos que realizó la AC IE, y afirmó que el fallo de TIC, al no respetar la obligación del responsable de verificar la validez de los procedimientos establecidos por su encargado del tratamiento, corresponde a una infracción del artículo 32 del RGPD (o el artículo 28 del RGPD, véase apartado anterior 6.2.4), y no del artículo 33, apartado 1, del RGPD. La AC FR argumenta que, si el encargado del tratamiento de TIC es su empresa matriz, «*era mucho más fácil para TIC verificar la validez de los procedimientos establecidos por la empresa matriz y exigir una corrección si era necesario*».

89. La **AC HU** formuló objeciones indicando que, dado el «defecto» de la aplicación de TIC a lo largo de los años y la gravedad de su naturaleza al afectar a la seguridad de los datos, la AC IE debería investigar si TIC también infringió el artículo 32 del RGPD sobre las obligaciones de TIC en cuanto a seguridad del tratamiento.

6.2.6 *Infracción del artículo 33, apartado 3, del RGPD sobre el contenido de la notificación de una violación de la seguridad de los datos personales en cuanto a la seguridad del tratamiento*

90. La **AC DE** expresó objeciones indicando que falta un examen de la AC IE relativo al alcance de la información que debe suministrarse en caso de una notificación, que se establece como vinculante en el artículo 33, apartado 3, del RGPD. A partir de los comentarios de TIC sobre la violación de la seguridad proporcionados conforme al artículo 33, apartado 5, del RGPD, y sobre la descripción de la investigación de los hechos del asunto, es obvio que TIC no cumplió plenamente su obligación de documentar cuando informó por primera vez de la violación de la seguridad el 8 de enero de 2019. La AC DE considera que, en este sentido, hay varios indicios de que el resultado también podría ser una infracción del artículo 33, apartado 3, del RGPD.

6.2.7 *Infracción del artículo 34 del RGPD sobre comunicación de una violación de la seguridad de los datos personales al interesado*

91. La **AC HU** formuló objeciones indicando que, dado el «defecto» de la aplicación de TIC a lo largo de los años y la gravedad de su naturaleza al afectar a la seguridad de los datos, la AC IE debería investigar si TIC también infringió el artículo 34 del RGPD sobre las obligaciones de TIC de informar a los interesados sobre la violación de la seguridad.

6.3 Posición de la ACP respecto a las objeciones

92. La ACP proporcionó su respuesta respecto a las objeciones relativas a posibles infracciones adicionales (o alternativas) del RGPD colectivamente en su Memorando colectivo compartido con las ACI. La ACP explicó que «*ejerció su discreción [...] para limitar el ámbito de la investigación a la consideración de dos cuestiones discretas, que eran si TIC había cumplido sus obligaciones como responsable en virtud del artículo 33, apartado 1, en relación con la notificación de la violación de la seguridad, y si había cumplido sus obligaciones conforme al artículo 33, apartado 5, de documentar la violación*»[91]. La ACP se basó en la sección 110(1) de la Ley en materia de protección de datos de Irlanda, de 2018, que dispone que la AC IE puede «*llevar a cabo la investigación de la forma que considere más conveniente*»[92]. La finalidad de la investigación, según la describe la AC IE, era «*exclusivamente examinar las circunstancias que rodean la notificación aparentemente retrasada de TIC respecto a la violación de la seguridad [...] y su forma de documentar la violación*», una cuestión que, en opinión de la AC IE, era «*de considerable importancia dado que, con cerca de 200 000 violaciones notificadas en dos años en toda la UE, existe la necesidad de aclarar sobre lo que se exige en una notificación de una violación y la documentación que debe presentarse conforme al RGPD*»[93].

93. En su Memorando colectivo[94], la AC IE mantiene que las objeciones formuladas en el contexto del artículo 60, apartado 4, del RGPD no pueden tener el efecto de cuestionar el alcance de una investigación. En el asunto en cuestión, la ACP recuerda que al inicio de la investigación informó a TIC de que su intención era verificar el cumplimiento de TIC conforme al artículo 33, apartados 1 y 5 del RGPD en relación con su notificación de una violación de la seguridad a la ACP el 8 de enero de 2019. Por lo tanto, el conjunto del proceso de investigación se llevó a cabo con este alcance, así como la

[91] Memorando colectivo, apartado 1.7.
[92] Memorando colectivo, apartado 1.5.
[93] Memorando colectivo, apartado 1.9.
[94] Memorando colectivo, apartado 5.44.

redacción del Proyecto de decisión, y se otorgó a TIC el derecho a ser oída en este sentido a cada paso del procedimiento. Por lo tanto, la ACP mantiene que si siguiera las objeciones de las ACI e incluyera otras infracciones en su decisión final «*solo en base al material contenido en el Proyecto de decisión*», el resultado sería que perjudicaría «*la totalidad de la investigación y el proceso del artículo 60 al exponerlo al riesgo de reclamaciones por falta de equidad procesal*»[95].

94. Asimismo, la ACP explica que tiene otra investigación en marcha en relación con otras violaciones de la seguridad de los datos que TIC notificó a la ACP con anterioridad a la notificación que afecta al presente asunto. En esta otra investigación, iniciada antes de la actual, la ACP destaca que el alcance de la investigación se refiere a un posible incumplimiento de los artículos 5, 24, 25, 28, 29 y 32 del RGPD, entre otros[96]. La ACP considera que, de hecho, en esta investigación paralela se intenta averiguar si TIC cumplió sus obligaciones más amplias según el RGPD, para determinar si las violaciones de la seguridad proceden de una falta de conformidad normativa. En consecuencia, la ACP opina que las ACI tendrán la posibilidad de considerar esas posibles infracciones en el contexto de dicha otra investigación, dado que serán consultadas respecto al correspondiente proyecto de decisión conforme al artículo 60, apartado 4, del RGPD[97].

95. TIC indica en su respuesta que, dado que el Proyecto de decisión señala que «*un examen detallado de las medidas técnicas y organizativas queda fuera del alcance de la investigación*[98]», y «*no sería razonable o apropiado, y ofendería los bien establecidos principios de la justicia natural, si la Decisión extrajera conclusiones o impusiera sanciones a TIC respecto a obligaciones y principios que no forman parte de la investigación de la ACP, dado que TIC no habría tenido oportunidad de responder a posibles dudas que la ACP o las ACI pudieran tener sobre los procesos de TIC en estos ámbitos*»[99].

6.4 Análisis del CEPD

6.4.1 Evaluación de si las objeciones son pertinentes y motivadas

6.4.1.1 Infracción del artículo 5, apartado 1, letra f), del RGPD sobre el principio de integridad y confidencialidad

96. El CEPD observa que la objeción de la **AC DE** sobre el artículo 5, apartado 1, letra f), del RGPD se refiere a si existe una infracción del RGPD y expresa un desacuerdo respecto a las conclusiones que pueden extraerse a partir del resultado de la investigación. La objeción también aporta argumentos para apoyar la conclusión de que debería valorarse la conformidad con el artículo 5, apartado 1, letra f), del RGPD. La objeción de la AC DE demuestra claramente la importancia de los riesgos que entraña el Proyecto de decisión para los derechos fundamentales de los interesados, en particular al destacar que los hechos constituyen una violación «significativa» y «sustancial» de la confidencialidad de los datos personales, y que un gran número de personas se vieron afectadas durante un período de tiempo sustancial. Además, la AC DE también argumenta que había indicios para considerar la existencia de

[95] Memorando colectivo, apartado 5.44 (c).
[96] Memorando colectivo, apartado 1.10.
[97] Memorando colectivo, apartado 5.44 (d).
[98] Proyecto de decisión, apartado 7.19.
[99] Declaraciones en respuesta a las objeciones y comentarios de las ACI, presentadas por TIC (14 de agosto de 2020), apartado 4.1. El CEPD desea destacar que la AC IE hizo llegar a TIC las objeciones formuladas por las ACI, y TIC redactó las declaraciones mencionadas sobre las objeciones, que fueron tenidas en cuenta por la AC IE antes de iniciar el procedimiento del artículo 65, y son parte del expediente objeto de consideración por el CEPD en el contexto de este procedimiento. Véase también la nota 19.

un «error sistémico» que habría requerido un examen más a fondo, más allá del defecto específico examinado.

97. La objeción de la **AC HU** también se puede considerar pertinente dado que afecta a si existe una infracción del RGPD. Además, (solo) hace una breve referencia a los argumentos de hecho respecto a la necesidad de evaluar esta disposición adicional (la duración del defecto y la gravedad de su naturaleza que afecta a la seguridad de los datos), pero no «demuestra claramente» la importancia de los riesgos que entraña el Proyecto de decisión para los derechos y libertades de las personas, dado que no aporta argumentos o justificaciones sobre las consecuencias de emitir una decisión sin los cambios propuestos en la objeción[100].

98. En consecuencia, el CEPD considera que la objeción formulada por la AC DE en relación con la posible infracción adicional del artículo 5, apartado 1, letra f) del RGPD es pertinente y motivada a efectos del artículo 4, apartado 24, del RGPD, pero considera que la objeción de la AC HU en relación con el mismo tema no cumple los requisitos del artículo 4, apartado 24[101].

99. El CEPD valorará el fondo de las cuestiones sustanciales planteadas por la objeción de la AC DE en relación con la posible infracción adicional del artículo 5, apartado 1, letra f) del RGPD (véase apartado 6.4.2 siguiente).

6.4.1.2 Infracción del artículo 5, apartado 2, del RGPD sobre el principio de responsabilidad proactiva

100. La objeción planteada por la **AC IT** debe considerarse «pertinente» porque, si se siguiera, comportaría una conclusión diferente respecto a si existe una infracción del RGPD[102]. Más específicamente, incluye un «desacuerdo sobre las conclusiones que deben extraerse de los resultados de la investigación», porque afirma que «*los resultados implican una infracción de una disposición del RGPD [...] además de [...] las ya analizadas en el Proyecto de decisión*»[103].

101. Asimismo, la objeción está «motivada» porque incluye aclaraciones sobre por qué se propone la modificación de la decisión[104]: el cambio propuesto se basa en «*la falta de políticas corporativas formalizadas para gestionar incidentes de seguridad [...] o el hecho de no cumplir dichas políticas*», y en el hecho de que «*[la AC IE] destaca estas deficiencias de procedimiento reiteradamente*» en el Proyecto de decisión, así como en la incapacidad del responsable del tratamiento de indicar el número exacto y la naturaleza de los datos personales e interesados afectados.

102. La **AC IT** demuestra claramente la importancia de los riesgos que entraña el Proyecto de decisión para los derechos y libertades fundamentales de los interesados, al demostrar «las implicaciones que el proyecto de decisión habría tenido para los valores protegidos»[105] y más concretamente el «impacto en los derechos y libertades de los interesados cuyos datos personales podrían ser objeto de

[100] Directrices sobre OPM, apartado 19.
[101] En consecuencia, el CEPD no se pronuncia sobre el fondo de ninguna cuestión sustancial planteada en la objeción de la AC HU. El CEPD reitera que su decisión actual se entiende sin perjuicio de posibles evaluaciones que se puedan requerir del CEPD en otros asuntos, incluso con las mismas partes, teniendo en cuenta el contenido del Proyecto de decisión en cuestión y las objeciones formuladas por las ACI.
[102] Directrices sobre OPM, apartado 13.
[103] Directrices sobre OPM, apartado 27.
[104] Directrices sobre OPM, apartado 17.
[105] Directrices sobre OPM, apartado 37.

tratamiento en el futuro»[106]: en la objeción se argumenta que los aspectos mencionados son «*estructurales en su naturaleza en lo que se refiere a la organización del responsable» y «sujetos a producir efectos no solamente en el asunto en cuestión, sino también en la gestión de otras violaciones de la seguridad de datos personales que puedan ocurrir en el futuro*».

103. En consecuencia, la objeción de la AC IT sobre el artículo 5, apartado 2, del RGPD satisface los requisitos establecidos en el artículo 4, apartado 24, del RGPD. El CEPD por lo tanto analizará el fondo de las cuestiones sustanciales planteadas en esa objeción[107].

6.4.1.3 Infracción del artículo 24 del RGPD sobre la responsabilidad del responsable del tratamiento

104. La objeción de la **AC DE** se refiere específicamente al apartado 5 del Proyecto de decisión[108], y se opone al Proyecto de decisión en cuando a si TIC infringió también el artículo 24 del RGPD[109]. Se basa en los hechos[110] establecidos en el Proyecto de decisión, de que «*si un usuario de Twitter con una cuenta protegida, que use Twitter para Android, cambiara su dirección electrónica, el defecto haría que su cuenta quedara desprotegida*»[111]. Y el servicio haría que sus tuiteos fueran públicos. Más precisamente, la AC DE cuestiona por qué la AC IE no examina, en el Proyecto de decisión, las causas de la violación, en particular a la luz del artículo 24 del RGPD, y por qué la AC IE no explica en el Proyecto de decisión el motivo por el que no realiza este examen.

105. La AC DE argumenta que, dado que la notificación de la violación mostraba «*deficiencias en la conformidad con el RGPD, ... [una] empresa que, por sus propios medios y recursos, mediante inspecciones de los equipos de seguridad internos y externos, no es capaz de encontrar un defecto de tal importancia y alcance, debería ser objeto de un escrutinio más profundo en cuanto a su seguridad y configuración de tratamiento de datos, más allá del defecto específico en cuestión*».

106. Según la AC DE, un escrutinio más a fondo de la configuración de tratamiento de datos de TIC «*podría derivar, según el caso, en una orden para que el responsable haga que las operaciones de tratamiento de datos sean conformes con lo dispuesto en el RGPD. El asunto en cuestión no refleja esta tarea. Y por eso es aún más urgente examinar el poder de corrección a la luz del artículo 58, apartado 2, del RGPD en este contexto*».

107. Por lo tanto, la AC DE indica lo que considera una ausencia de evaluación, con las consecuencias de que las conclusiones extraídas de los resultados de la investigación por parte de ACP podrían ser distintas[112].

108. La AC DE argumenta que «*según el artículo 83, apartado 1, del RGPD las sanciones deben ser «efectivas, proporcionadas y disuasorias. en cada asunto individual. Una sanción es efectiva y disuasoria si, por una parte, es adecuada como medida preventiva general para disuadir al público en general de cometer infracciones y reafirmar la confianza de la población en general en la validez del Derecho de la Unión, pero, por otro lado, también es adecuada como medida preventiva para disuadir al infractor de cometer nuevas infracciones*». En consecuencia, la AC DE demuestra que el hecho de no

[106] Directrices sobre OPM, apartado 43.
[107] Véase el apartado 6.4.2 más adelante.
[108] Directrices sobre OPM, apartado 20.
[109] Directrices sobre OPM, apartado 12.
[110] Directrices sobre OPM, apartado 14.
[111] Proyecto de decisión, apartado 2.7.
[112] Directrices sobre OPM, apartado 29.

cambiar el Proyecto de decisión para que incluya una evaluación de la conformidad con el artículo 24 del RGPD implicaría un riesgo considerable para los derechos y libertades fundamentales de los interesados[113].

109. En sus Directrices sobre OPM, el CEPD acepta que una objeción puede cuestionar la conclusión de la ACP, considerando que los resultados de la ACP en realidad llevan a la conclusión de que se ha infringido otra disposición del RGPD además de, o en vez de, la disposición identificada por la ACP[114]. El CEPD considera que esta es precisamente la esencia de la objeción de la AC DE, lo que no impide que sea pertinente y motivada.

110. Además, la objeción de la AC DE demuestra claramente la importancia de los riesgos que entraña el Proyecto de decisión para los derechos y libertades de los interesados, por ejemplo destacando que se vieron afectadas un gran número de personas durante un período de tiempo prolongado, lo que refleja un error sistémico que exige un escrutinio más a fondo, más allá del defecto específico en cuestión. En consecuencia, la objeción de la AC DE sobre el artículo 24 del RGPD satisface los requisitos establecidos en el artículo 4, apartado 24, del RGPD.

111. En vista del análisis efectuado, el CEPD considera que la objeción de la AC DE relativa a una posible infracción del artículo 24 del RGPD es pertinente y razonada conforme al artículo 4, apartado 24 del RGPD. En consecuencia, el CEPD evaluará el fondo de las cuestiones sustanciales planteadas en esta objeción (véase apartado 6.4.2 más adelante).

6.4.1.4 Infracción del artículo 28 del RGPD sobre la relación con los encargados del tratamiento

112. La objeción de la **AC FR** se refiere específicamente a los apartados 7.129 iii), iv) y v) del Proyecto de decisión[115], y cuestiona el Proyecto de decisión en relación con si TIC infringió el artículo 28 del RGPD en vez del artículo 33, apartado 1, del RGPD[116]. Se basa en los hechos[117] establecidos en el Proyecto de decisión y en el hecho de que la ACP concluyera que «TIC no respetó la obligación del responsable de verificar la validez de los procedimientos establecidos por su encargado».

113. Según la AC FR, dado que el artículo 28, apartado 3, letra h), del RGPD establece las obligaciones del responsable del tratamiento cuando utiliza a un encargado, los resultados deberían haber llevado a la ACP a la conclusión de que se infringió el artículo 28, apartado 3, letra h), del RGPD en vez del artículo 33, apartado 1, del RGPD. En definitiva, en opinión de la AC FR, esto significa que la sanción en forma de multa debería abordar diferentes infracciones.

114. En sus Directrices sobre OPM, el CEPD acepta que una objeción puede cuestionar la conclusión de la ACP, considerando que los resultados de la ACP en realidad llevan a la conclusión de que se ha infringido otra disposición del RGPD además de, o en vez de, la disposición identificada por la ACP[118]. El CEPD considera que esta es precisamente la esencia de la objeción de la AC FR, lo que no impide que sea pertinente. Además, la objeción aporta argumentos adecuados a favor de la conclusión propuesta. Al mismo tiempo, el CEPD observa que la objeción de la AC FR no demuestra claramente los riesgos importantes que entraña el Proyecto de decisión para los derechos y libertades fundamentales de los

[113] Directrices sobre OPM, apartado 19.
[114] Directrices sobre OPM, apartado 27.
[115] Directrices sobre OPM, apartado 20.
[116] Directrices sobre OPM, apartado 12.
[117] Directrices sobre OPM, apartado 14.
[118] Directrices sobre OPM, apartado 27.

interesados en relación con el hecho de no considerar la infracción de esta disposición específica[119]. A la luz del análisis efectuado, el CEPD considera que la objeción de la AC FR relativa a una posible infracción del artículo 28 del RGPD en vez del artículo 33, apartado 1, del RGPD no es pertinente y razonada conforme al artículo 4, apartado 24 del RGPD.

115. La AC IT se opone al Proyecto de decisión en el sentido de si TIC infringió o no el artículo 28 del RGPD, entre otros, además del artículo 33, apartado 1, del RGPD[120].

116. La AC IT se basa en los hechos establecidos en el Proyecto de decisión y en las conclusiones de la ACP de que, a pesar de que en las políticas internas de TIC se prevé la implicación del DPD global en el equipo de respuesta y detección de su encargado, Twitter, Inc., en la práctica el DPD no fue convocado. La AC IT observa también que Twitter, Inc., como encargado del tratamiento, no asistió correctamente a TIC.

117. Según la AC IT, dado que el artículo 28, apartado 1, del RGPD requiere a los responsables del tratamiento que solo utilicen encargados que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, y el artículo 28, apartado 3, letra f), del RGPD requiere que el contrato entre el responsable y el encargado disponga que el encargado ayudará «al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado»; los resultados tendrían que haber llevado a la ACP a la conclusión de que se habían infringido también el artículo 28, apartado 1, y el artículo 28, apartado 3, letra f) del RGPD.

118. El CEPD considera que la objeción formulada por la AC IT en relación con el artículo 28, apartado 1, y el artículo 28, apartado 3, letra f), del RGPD, debe considerarse «pertinente» porque, si se siguiera, comportaría una conclusión diferente respecto a si existe una infracción del RGPD[121]. Más específicamente, incluye un «desacuerdo sobre las conclusiones que deben extraerse de los resultados de la investigación», porque afirma que «los resultados implican una infracción de una disposición del RGPD [...] además de [...] las ya analizadas en el Proyecto de decisión»[122].

119. Asimismo, según el CEPD, la objeción está «motivada» porque incluye aclaraciones de por qué se propone la enmienda de la decisión[123]: el cambio propuesto se basa en el hecho de que el responsable no cumplió sus políticas internas según las cuales se debería haber llamado al DPD de TIC. Además, la objeción plantea la cuestión de que el encargado no cumplió su obligación contractual de ayudar al responsable con arreglo al artículo 28, apartado 3, letra f), del RGPD.

120. Sin embargo, el CEPD observa que la objeción de la AC IT relativa al artículo 28, apartado 1, y al artículo 28, apartado 3, letra f), del RGPD no demuestra claramente qué riesgos significativos entraña el Proyecto de decisión para los derechos y libertades fundamentales de los interesados[124]. En consecuencia, esta objeción formulada por la AC IT no satisface los requisitos establecidos en el artículo 4, apartado 24, del RGPD[125].

[119] Directrices sobre OPM, apartado 29.
[120] Directrices sobre OPM, apartado 12.
[121] Directrices sobre OPM, apartado 13.
[122] Directrices sobre OPM, apartado 27.
[123] Directrices sobre OPM, apartado 17.
[124] Directrices sobre OPM, apartado 29.
[125] En consecuencia, el CEPD no se pronuncia sobre el fondo de ninguna cuestión sustancial planteada en dichas objeciones. El CEPD reitera que su decisión actual es sin perjuicio de posibles evaluaciones que se puedan

6.4.1.5 Infracción del artículo 32 del RGPD sobre la seguridad del tratamiento

121. La objeción de la **AC DE**, si se siguiera, implicaría un cambio en la conclusión de si existe una infracción del RGPD, dado que identifica «*un desacuerdo en cuanto a las conclusiones que se pueden extraer de los resultados de la investigación*»[126] al señalar que los resultados pueden indicar una infracción también del artículo 32 del RGPD. Así, el CEPD considera que existe una relación entre el contenido de la objeción y una posible conclusión diferente[127]. Además, esta objeción está relacionada con el contenido de hecho y de Derecho específico del Proyecto de decisión[128].

122. Además, la objeción de la AC DE demuestra claramente la importancia de los riesgos que entraña el Proyecto de decisión para los derechos fundamentales de los interesados, en particular al destacar que los hechos constituyen una violación «significativa» y «sustancial» de la confidencialidad de los datos personales, y que un gran número de personas se vieron afectadas durante un período de tiempo sustancial. La AC DE también argumenta que hay indicios para considerar la existencia de un «error sistémico» que habría requerido un examen más a fondo, más allá del defecto específico examinado.

123. A la luz del análisis efectuado, el CEPD considera que la objeción de la AC DE relativa a una posible infracción del artículo 32 del RGPD es pertinente y razonada conforme al artículo 4, apartado 24 del RGPD. En consecuencia, el CEPD evaluará el fondo de las cuestiones sustanciales planteadas en esta objeción (véase apartado 6.4.2 más adelante).

124. En cuanto a la objeción de la **AC FR**, el CEPD considera que satisface el criterio de «pertinente» porque si la ACP la hubiera seguido, la conclusión sobre si ha habido infracción del RGPD habría sido distinta[129]. La objeción de la AC FR se basa en el razonamiento proporcionado por la AC IE en su Proyecto de decisión, y este razonamiento está relacionado con la conclusión de si se ha identificado correctamente una infracción del RGPD[130]. El CEPD recuerda que la ACI tiene que presentar los hechos que presuntamente lleven a una conclusión diferente[131] y observa que en el asunto en cuestión la objeción analiza los hechos que comportarían una infracción del artículo 32, apartado 1, letra d) del RGPD en vez de una infracción del artículo 33, apartado 1, del RGPD, y lo hace de forma coherente, clara y precisa, indicando claramente con qué partes de la decisión de la AC IE no está de acuerdo. La objeción de la AC FR es claramente pertinente porque describe un desacuerdo sobre si ha habido una infracción del RGPD. Sin embargo, la objeción de la AC FR explica solo sucintamente las razones del cambio que propone y no demuestra claramente la importancia de los riesgos que el Proyecto de decisión entraña en cuanto a los derechos y libertades de los interesados en caso de que no se tenga en cuenta esta infracción del artículo 32 del RGPD. En consecuencia, esta objeción formulada por la AC FR no satisface los requisitos establecidos en el artículo 4, apartado 24, del RGPD[132].

requerir del CEPD en otros asuntos, incluso con las mismas partes, teniendo en cuenta el contenido del Proyecto de decisión en cuestión y las objeciones formuladas por las ACI.

[126] Directrices sobre OPM, apartado 28.

[127] Directrices sobre OPM, apartado 13.

[128] Directrices sobre OPM, apartado 14.

[129] Directrices sobre OPM, apartado 13.

[130] Directrices sobre OPM, apartado 16.

[131] Directrices sobre OPM, apartado 18.

[132] En consecuencia, el CEPD no se pronuncia sobre el fondo de ninguna cuestión sustancial planteada en dichas objeciones. El CEPD reitera que su decisión actual se entiende sin perjuicio de posibles evaluaciones que se puedan requerir del CEPD en otros asuntos, incluso con las mismas partes, teniendo en cuenta el contenido del Proyecto de decisión en cuestión y las objeciones formuladas por las ACI.

125. La objeción de la **AC HU** también se refiere a si existe una infracción del RGPD argumentando que debería investigarse la posible infracción del principio de integridad y confidencialidad. La objeción de la AC HU es claramente relevante porque establece que debería haberse investigado una disposición adicional del RGPD (es decir, el artículo 32 del RGPD). Sin embargo, la AC HU no explica de qué modo el Proyecto de decisión comportaría algún riesgo, ni explica claramente por qué determinados aspectos de la decisión son deficientes desde este punto de vista[133]. La objeción de la AC HU no cumple el criterio de aportar un razonamiento sólido para esta objeción, con la aportación de argumentos de hecho o de Derecho. En cambio, solamente recomienda a la AC IE que debe investigarse el cumplimiento del artículo 32 del RGPD por parte del responsable del tratamiento. En consecuencia, esta objeción formulada por la AC HU no satisface los requisitos establecidos en el artículo 4, apartado 24, del RGPD[134].

6.4.1.6 Infracción del artículo 33, apartado 3, del RGPD sobre el contenido de la notificación de una violación de la seguridad de los datos personales en cuanto a la seguridad del tratamiento

126. La **AC DE** considera que el Proyecto de decisión indica que se podría haber infringido el artículo 33, apartado 3, del RGPD además de otras disposiciones del mismo Reglamento. En este sentido, trata de «si ha habido una infracción» del RGPD, y de que la misma no se examina ni se aborda en el Proyecto de decisión. Por este motivo, la AC DE considera que, si se cambiara, el Proyecto de decisión, se llegaría a la conclusión de que ha habido infracciones adicionales del RGPD.

127. Sin embargo, la AC DE no demuestra claramente la importancia de los riesgos que entraña el Proyecto de decisión para los derechos y libertades fundamentales de los interesados. En consecuencia, la objeción de la AC DE sobre el artículo 33, apartado 3, no cumple los requisitos establecidos en el artículo 4, apartado 24, del RGPD[135].

6.4.1.7 Infracción del artículo 34 del RGPD sobre comunicación de una violación de la seguridad de los datos personales al interesado

128. La **AC HU** considera que el Proyecto de decisión indica que se podría haber infringido el artículo 34 del RGPD además de otras disposiciones del RGPD, especialmente por el hecho de que el defecto perduró a lo largo de los años, y dada la gravedad del efecto en la seguridad del responsable del tratamiento. En este sentido, trata de «si ha habido una infracción» del RGPD, y de que la misma no se examina ni se aborda en el Proyecto de decisión. Por este motivo, la AC HU considera que, si se cambiara, el Proyecto de decisión llevaría a la conclusión de que ha habido infracciones adicionales del RGPD.

129. Sin embargo, la AC HU no demuestra claramente la importancia de los riesgos que entraña el Proyecto de decisión para los derechos y libertades fundamentales de los interesados. En consecuencia, la

[133] Directrices sobre OPM, apartado 18.

[134] En consecuencia, el CEPD no se pronuncia sobre el fondo de ninguna cuestión sustancial planteada en dichas objeciones. El CEPD reitera que su decisión actual se entiende sin perjuicio de posibles evaluaciones que se puedan requerir del CEPD en otros asuntos, incluso con las mismas partes, teniendo en cuenta el contenido del Proyecto de decisión en cuestión y las objeciones formuladas por las ACI.

[135] En consecuencia, el CEPD no se pronuncia sobre el fondo de ninguna cuestión sustancial planteada en dichas objeciones. El CEPD reitera que su decisión actual se entiende sin perjuicio de posibles evaluaciones que se puedan requerir del CEPD en otros asuntos, incluso con las mismas partes, teniendo en cuenta el contenido del Proyecto de decisión en cuestión y las objeciones formuladas por las ACI.

objeción de la AC HU sobre el artículo 34 del RGPD no cumple los requisitos establecidos en el artículo 4, apartado 24, del RGPD[136].

6.4.2 Evaluación del fondo de las cuestiones sustanciales planteadas en las objeciones pertinentes y motivadas y conclusión

130. El Comité analizará a continuación las objeciones que se han considerado pertinentes y motivadas, en concreto las objeciones de la AC DE sobre el artículo 5, apartado 1, letra f), los artículos 24 y 32 del RGPD, así como la objeción de la AC IT sobre el artículo 5, apartado 2, del RGPD, además de la respuesta de la ACP a dichas objeciones y las alegaciones de TIC.

131. Conforme al artículo 65, apartado 1, letra a), del RGPD, en el contexto de un procedimiento de resolución de conflictos, el CEPD debe emitir una decisión vinculante en todos los asuntos que sean objeto de objeciones motivadas y pertinentes, en particular si existe una infracción del RGPD. El CEPD puede (y debe) tomar una decisión vinculante que, siempre que sea posible, tenga en cuenta los elementos del expediente y el derecho del demandado a ser escuchado, y proporcionar una conclusión final sobre la aplicación del RGPD en relación con el asunto en cuestión. Entonces, la ACP estará obligada a implementar los cambios en su decisión final.

132. El Comité considera que los elementos de hecho disponibles incluidos en el Proyecto de decisión y en las objeciones no son suficientes para que el CEPD pueda establecer la existencia de infracciones adicionales (o alternativas) del artículo 5, apartado 1, letra f), el artículo 5, apartado 2, y los artículos 24 y 32 del RGPD.

133. El Comité considera que, en general, el alcance limitado de la investigación efectuada por la AC IE —centrada desde el inicio solo en si TIC había infringido el artículo 33, apartados 1 y 5, del RGPD— afecta directamente al fondo de la investigación y la posibilidad de encontrar más hechos, así como la capacidad de las ACI de presentar suficientes elementos para que el CEPD defienda las objeciones.

134. El CEPD recuerda la obligación de la ACP de «esforzarse para llegar a un consenso» con las ACI (artículo 60, apartado 1, del RGPD) y proporcionar, sin dilación, a las ACI «la información pertinente» sobre el asunto (artículo 60, apartado 3, del RGPD). Incluso en el caso de una investigación por iniciativa propia, las Directrices sobre objeciones pertinentes y motivadas establecen que la ACP «debe buscar el consenso respecto al alcance del procedimiento (es decir, los aspectos del tratamiento de datos bajo escrutinio) antes de iniciar el procedimiento formalmente»[137], incluso en el contexto de un nuevo posible procedimiento.

135. Aunque el CEPD considera que las AC gozan de un cierto grado de discreción para decidir cómo enmarcar el alcance de sus investigaciones, el CEPD recuerda que uno de los principales objetivos del RGPD es garantizar la coherencia en toda la Unión Europea, y la cooperación entre la ACP y las ACI es uno de los medios para conseguirlo. El CEPD también recuerda que el RGPD proporciona toda una gama de herramientas de cooperación (por ejemplo en los artículos 61 y 62 del RGPD), teniendo en cuenta el objetivo de llegar al consenso dentro del mecanismo de cooperación y la necesidad de intercambiar toda la información pertinente, de cara a garantizar la protección de los derechos y libertades fundamentales de los interesados.

[136] En consecuencia, el CEPD no se pronuncia sobre el fondo de ninguna cuestión sustancial planteada en dichas objeciones. El CEPD reitera que su decisión actual se entiende sin perjuicio de posibles evaluaciones que se puedan requerir del CEPD en otros asuntos, incluso con las mismas partes, teniendo en cuenta el contenido del Proyecto de decisión en cuestión y las objeciones formuladas por las ACI.
[137] Directrices sobre OPM, apartado 28.

136. El CEPD considera que al determinar el alcance de la investigación, si bien puede ser limitado, la ACP debe delimitarlo de tal manera que permita a las ACI cumplir de forma eficiente su función, junto con la ACP, al determinar si ha habido una infracción del RGPD.

7 SOBRE LAS MEDIDAS CORRECTIVAS DECIDIDAS POR LA ACP, EN PARTICULAR LA IMPOSICIÓN DE UNA SANCIÓN CON APERCIBIMIENTO

7.1 Análisis de la ACP en el Proyecto de decisión

137. En el Proyecto de decisión se explica que, a pesar de que en el Proyecto de decisión preliminar las medidas correctivas que se querían imponer eran un apercibimiento (conforme al artículo 58, apartado 2, letra b), del RGPD) y una multa administrativa (conforme al artículo 58, apartado 2, letra i), del RGPD), el Proyecto de decisión final consiste en la imposición solo de una multa administrativa a TIC como responsable del tratamiento[138].

138. En sus alegaciones en relación con el Proyecto de decisión preliminar, TIC cuestionaba la decisión de emitir un apercibimiento, argumentando que las infracciones del artículo 33, apartados 1 y 5, del RGPD no incluían «operaciones de tratamiento», mientras que el artículo 58, apartado 2, letra b) del RGPD otorga a las autoridades de control el poder de sancionar con apercibimiento cuando se han infringido disposiciones sobre operaciones de tratamiento del RGPD[139]. El argumento de TIC se basa principalmente en el hecho de que ni el retraso en notificar a la AC ni el hecho de no conservar los registros adecuados constituye una operación de tratamiento por sí misma[140].

139. En su Proyecto de decisión, la AC IE explica su decisión de no emitir un apercibimiento, recordando el argumento planteado por TIC en sus alegaciones en relación con el Proyecto de decisión preliminar, donde argumenta que las infracciones del artículo 33, apartados 1 y 5, del RGPD no incluyen las «operaciones de tratamiento», mientras que el artículo 58, apartado 2, letra b), del RGPD otorga a las autoridades de control el poder de sancionar con apercibimiento cuando se han infringido disposiciones sobre operaciones de tratamiento del RGPD[141]. La AC IE observa que la expresión «operación(es) de tratamiento» aparece 50 veces en el RGPD y parece ser que se utiliza para referirse al tratamiento o el uso de (o, en otras palabras, cosas que se hacen para) datos personales controlados por un responsable del tratamiento, pero al mismo tiempo observa que la definición de «tratamiento» que proporciona el RGPD es muy amplia, lo que, dado que una violación es algo que afecta o que se hace a los datos personales, permite deducir que la obligación de notificación (en la medida en que implica inherentemente un examen de lo que ha ocurrido con datos personales, o cómo ha afectado a los datos personales) está intrínsecamente relacionada con una o más operaciones de tratamiento[142]. La AC IE, en su Proyecto de decisión, no considera necesario llegar a una conclusión definida del significado y el efecto de la expresión «operaciones de tratamiento» pero «en conjunto» considera

[138] Proyecto de decisión, apartado 12.1.
[139] Alegaciones de TIC en relación con el Proyecto de decisión preliminar, apartado 11.1.
[140] Proyecto de decisión, apartado 12.4.
[141] Alegaciones de TIC en relación con el Proyecto de decisión preliminar, apartado 11.1.
[142] Proyecto de decisión, apartado 12.5.

que el argumento jurídico de TIC es «un argumento aceptable» y decide no proceder con la adopción de una sanción con apercibimiento para TIC[143].

7.2 Resumen de las objeciones formuladas por las ACI

140. La **AC DE** formuló una objeción sobre el hecho de que, aunque en el Proyecto de decisión preliminar se preveía un apercibimiento y una multa administrativa, solo se incluya una multa administrativa en el Proyecto de decisión. La AC DE no está de acuerdo con el razonamiento presentado por la AC IE sobre la decisión de no imponer una sanción con apercibimiento. Según la AC DE, el razonamiento jurídico que la ACP considera «aceptable» no es convincente dado que la interpretación jurídica requiere no solo un examen de los términos de la disposición sino también de su significado y su propósito, la historia de su desarrollo y su integración sistemática en la totalidad del complejo regulador.

7.3 Posición de la ACP respecto a las objeciones

141. En su Memorando colectivo, la AC IE considera que, a pesar de que la objeción de la AC DE se refiere a «si la actuación prevista en relación con un responsable o un encargado cumple [el RGPD]», no demuestra que el hecho de no emitir una sanción con apercibimiento a TIC puede entrañar riesgos importantes para los interesados[144] en cuanto a que la decisión de no emitir un apercibimiento no es pertinente y motivada conforme al artículo 4, apartado 24, del RGPD.

142. Sin embargo, al abordar el fondo de las cuestiones sustanciales planteadas en las objeciones, la ACP explica que considera la expresión «operaciones de tratamiento» conforme a su significado y aplicación en todo el RGPD, y observa que esta expresión solo se utiliza para las facultades de las AC en el artículo 58 del RGPD. Tras las alegaciones de TIC a las objeciones de las ACI sobre este punto, y teniendo en cuenta que el alcance de la investigación se centraba en las obligaciones del responsable del tratamiento en relación con la notificación de la violación, la ACP decidió que su investigación «*no daba como resultado que las "operaciones de tratamiento" subyacentes en relación con la violación de la seguridad infringieran [...] el RGPD*»[145]. Por lo tanto, la ACP consideró que no había motivos para revisar la decisión de no emitir una sanción con apercibimiento a la luz de la objeción de la AC DE.

143. La ACP observó que su postura en el Proyecto de decisión de no emitir una sanción con apercibimiento solo es aplicable a las circunstancias específicas de este asunto; por ello, se entiende sin perjuicio de futuras decisiones sobre apercibimientos que la ACP u otras ACI puedan tomar[146].

7.4 Análisis del CEPD

7.4.1 Evaluación de si las objeciones son pertinentes y motivadas

144. La objeción de la **AC DE** se refiere a la conformidad de la actuación prevista con el RGPD, dado que indica qué acción correctiva sería adecuada, en su opinión, para que la ACP la incluyera en la decisión final: por lo tanto, se trata de una objeción pertinente, que muestra adecuadamente la conclusión

[143] Proyecto de decisión, apartado 12.5. El resto de argumentos independientes presentados por TIC en relación con por qué no se considera apropiada la imposición de un apercibimiento (ver alegaciones de TIC en relación con el Proyecto de decisión preliminar, apartados 11.2-11.4) no se consideraron por separado a la luz de la decisión ya mencionada (Proyecto de decisión, apartado 12.6).
[144] Memorando colectivo, apartado 5.79.
[145] Memorando colectivo, apartado 5.78.
[146] Memorando colectivo, apartado 5.78.

diferente que se propone. Además, incluye un razonamiento jurídico que respalda esta opinión y propone una interpretación jurídica alternativa. No obstante, la objeción no demuestra claramente la importancia del riesgo que entraña el Proyecto de decisión para los derechos y libertades de los interesados y/o la libre circulación de datos personales. En concreto, no aporta una motivación sobre cómo el hecho de no imponer una sanción con apercibimiento en este asunto específico —en el que ya se impone una multa administrativa— podría suponer un riesgo para los derechos y libertades fundamentales de los interesados.

7.4.2 Conclusión

145. El CEPD considera que esta objeción no cumple los requisitos del artículo 4, apartado 24, del RGPD.

146. El CEPD observa que su postura respecto a la decisión de la ACP de no emitir una sanción con apercibimiento solo es aplicable a las circunstancias específicas de este asunto; por ello, se entiende sin perjuicio de futuras decisiones sobre apercibimientos por parte de la ACP u otras ACI[147].

147. Como ya se ha dicho, la decisión del CEPD de no evaluar el fondo del contenido de la objeción planteada se entiende sin perjuicio de futuras decisiones del CEPD sobre las mismas cuestiones o similares.

8 SOBRE LAS MEDIDAS CORRECTIVAS, EN PARTICULAR EL CÁLCULO DE LA MULTA ADMINISTRATIVA

8.1 Análisis de la ACP en el Proyecto de decisión

148. El Proyecto de decisión explica que la AC IE tuvo en cuenta los criterios del artículo 83, apartado 2, del RGPD al decidir si debía imponer una multa administrativa y cómo determinar su importe[148].

149. En lo que se refiere al cálculo de la multa, el Proyecto de decisión analiza, en primer lugar, **la naturaleza, gravedad y duración de la infracción**, conforme al artículo 83, apartado 2, letra a), del RGPD[149]. El Proyecto de decisión tuvo en cuenta la «*naturaleza, el alcance o la finalidad del tratamiento*» al referirse a la naturaleza de las operaciones de tratamiento llevadas a cabo por Twitter (una plataforma social de «microblogging» en la que los usuarios pueden expresar sus pensamientos en forma de tuiteos o «tweets»), a la naturaleza del tratamiento que dio lugar a la violación de la seguridad (derivada de un defecto que hizo que los tuiteos antes «protegidos» quedaran «desprotegidos» y accesibles para todo el mundo en aquellos casos en los que los usuarios de Android habían cambiado su dirección electrónica), y al alcance del tratamiento (el derecho afectó al menos a 88 726 usuarios de la UE/EEE, dado que otras personas adicionales se vieron afectadas entre la fecha del defecto, el 4 de noviembre de 2014, y la fecha de su reparación total, el 14 de enero de 2019, pero no ha sido posible identificarlas a todas)[150].

[147] Memorando colectivo, apartado 5.78.
[148] Proyecto de decisión, apartados 14.1-14.62.
[149] El artículo 83, apartado 2, letra a), del RGPD se refiere a «*la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, 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*».
[150] Proyecto de decisión, apartado 14.2.

150. El Proyecto de decisión también tuvo en cuenta **el número de interesados afectados y la gravedad de los daños sufridos**[151] al concluir que el número de interesados que podrían haberse visto potencialmente afectados por el retraso en la notificación y el posible daño a los interesados derivado del consecuente retraso en la evaluación por parte de la AC eran factores pertinentes que debían tenerse en cuenta[152]. Se recuerda que el impacto en los usuarios individuales y la posibilidad de daños derivados de todo ello influirá en el nivel y la naturaleza de los datos personales que se hagan públicos, y que existía al menos un potencial de daños a los interesados vinculado al retraso en las acciones correctivas[153]. La postura de la AC IE en el Proyecto de decisión preliminar era que «*aunque TIC no había confirmado la naturaleza precisa de los datos hechos públicos debido a la violación de la seguridad, era razonable deducir que, dada la escala de los usuarios afectados y la naturaleza del servicio ofrecido por TIC, algunos de los datos personales publicados en relación con, al menos, algunos de los usuarios pertenecían a categorías de datos sensibles y otro material especialmente privado*»[154]. Esta postura quedó matizada en el Proyecto de decisión a la luz de la respuesta de TIC, dado que la AC IE decidió que «*debe atribuirse menos peso a este factor*», basándose en el hecho de que «*aunque no puede decirse definitivamente que ningún usuario afectado por la violación se vio afectado por el retraso en la notificación, no hay pruebas directas de daños a los interesados derivados del retraso en la notificación*»[155].

151. En relación con la **naturaleza de la infracción**, el Proyecto de decisión destaca que las infracciones del artículo 33, apartados 1 y 5, del RGPD no tienen ninguna relación con la cuestión sustantiva de la violación[156]. La AC IE también consideró que la naturaleza de las obligaciones derivadas del artículo 33, apartados 1 y 5, del RGPD es tal que el cumplimiento es esencial para el funcionamiento global del régimen de supervisión y ejecución implantado por las autoridades de control en relación tanto con la cuestión específica de las violaciones de la seguridad de los datos personales, como la identificación y evaluación de cuestiones más amplias de incumplimiento por parte de los responsables del tratamiento, y que el incumplimiento de dichas obligaciones tiene graves consecuencias porque se corre el riesgo de socavar el ejercicio efectivo por parte de las AC de sus funciones conforme al RGPD[157].

152. En relación con la **gravedad de la infracción** del artículo 33, apartado 1, del RGPD, el Proyecto de decisión tuvo en cuenta el modo como interfirió con la finalidad general de notificar una violación de la seguridad de los datos personales a la autoridad de control, el hecho de que no se observaron daños materiales a los interesados, el hecho de que las medidas de reparación por parte de TIC se limitaron a la acción de reparar el defecto (y no se realizó un análisis retroactivo para identificar los riesgos para los interesados debidos a la violación), y el hecho aparente de que TIC no realizó una evaluación formal del riesgo[158]. En el Proyecto de decisión no se tiene en cuenta la afirmación de TIC de que la violación fue debida a un fallo aislado (que comportó el retraso en la notificación al DPD) de suficiente peso como para atenuar la gravedad de la infracción (pero sí se tuvo en cuenta dicha naturaleza de incidente aislado, a partir de la opinión provisional del Proyecto preliminar de que la violación era un indicio de

[151] Proyecto de decisión, apartados 14.3-14.5.
[152] Proyecto de decisión, apartado 14.5.
[153] Proyecto de decisión, apartado 14.5 (en el Proyecto de decisión se indica que «es evidente que el impacto en cada uno de los usuarios, y la posibilidad de daños derivados de todo ello, dependerá del nivel de datos personales que se hagan públicos y, también, de la naturaleza de dichos datos personales»).
[154] Proyecto de decisión, apartado 14.5.
[155] Proyecto de decisión, apartado 14.5.
[156] Proyecto de decisión, apartado 14.6.
[157] Proyecto de decisión, apartado 14.11.
[158] Proyecto de decisión, apartados 14.16-14.18.

un problema más amplio y más sistémico)[159]. En cuanto a la gravedad de la infracción del artículo 33, apartado 5, del RGPD, el Proyecto de decisión destacaba que era necesario documentar adecuadamente las infracciones para que la autoridad de control pudiera verificar que el responsable del tratamiento había cumplido el artículo 33, apartado 5, del RGPD[160], y que la AC IE tuvo que realizar varias consultas para conseguir aclarar los hechos relativos a la notificación de la violación[161],pero reconoció que las deficiencias en la documentación se debían a un malentendido sin mala fe de los requisitos (que, no obstante, quedan claros a partir del redactado de la disposición)[162]. El Proyecto de decisión concluía que cada infracción era de un grado «*bajo a moderado en la escala de gravedad*»[163].

153. En relación con la **duración de la infracción** del artículo 33, apartado 1, del RGPD, en el Proyecto de decisión se comenta que se trataba de un período de dos días y se evalúa a la luz del plazo general normalmente permitido para las notificaciones de violaciones (72 horas), teniendo en cuenta que no se trataba de una infracción trivial o sin consecuencias[164]. En cuanto a la duración de la infracción del artículo 33, apartado 5, del RGPD, en el Proyecto de decisión se llega a la conclusión de que sigue en curso[165].

154. En relación con el **artículo 83, apartado 2, letra b), del RGPD** (el carácter intencionado o negligente de la infracción), la AC IE concluye en su Proyecto de decisión que hubo un **carácter negligente** en la infracción de TIC del artículo 33, apartado 1, del RGPD[166], y destaca que el retraso en la notificación al DPD global ocurrió porque una parte del protocolo interno de Twitter Group no se cumplió como estaba prescrito y no era tan claro como debería haber sido[167]. Esto llevó a la conclusión de que el retraso se produjo como resultado de una negligencia por parte del responsable del tratamiento, pero se aceptó la alegación de TIC de que el retraso de la notificación no era indicativo de una cuestión sistémica más amplia y fue un hecho aislado[168]. La AC IE no identificó ninguna prueba de conducta intencionada en relación con la infracción del artículo 33, apartado 1, del RGPD[169]. El Proyecto de decisión también identificó que hubo un carácter negligente en la infracción de TIC del artículo 33, apartado 5, del RGPD[170], porque no había conocimiento ni voluntad de causar la infracción (que habría sido equivalente a intencionada) sino que la documentación no era suficiente para permitir la verificación del cumplimiento del artículo 33[171].

155. En cuanto al **artículo 83, apartado 2, letra c) del RGPD**, es decir la actuación del responsable del tratamiento para **mitigar el daño sufridos por los interesados**, el Proyecto de decisión consideró que se habían tomado medidas reparadoras para evitar la repetición del problema y rectificar el defecto,

[159] Proyecto de decisión, apartado 14.19.
[160] Proyecto de decisión, apartado 14.20.
[161] Proyecto de decisión, apartado 14.21.
[162] Proyecto de decisión, apartado 14.24.
[163] Proyecto de decisión, apartado 14.24.
[164] Proyecto de decisión, apartado 14.26 (empezó en la expiración de las 72 horas, desde el 3 de enero de 2019) (es decir el 6 de enero de 2019) y acabó en el momento en que TIC comunicó la violación de la seguridad el 8 de enero de 2019.
[165] Proyecto de decisión, apartado 14.29.
[166] Proyecto de decisión, apartado 14.34.
[167] Proyecto de decisión, apartados 14.33-14.34.
[168] Proyecto de decisión, apartado 14.34.
[169] Proyecto de decisión, apartado 14.35.
[170] Proyecto de decisión, apartado 14.38.
[171] Proyecto de decisión, apartados 14.36, 14.38.

lo que se consideró como único factor atenuante al valorar el importe de la multa que debía imponerse[172].

156. El Proyecto de decisión considera que el **Artículo 83, apartado 2, letra d) del RGPD**, es decir, el **grado de responsabilidad** del responsable o del encargado del tratamiento, detallando las medidas técnicas y organizativas existentes, y posteriormente mejoradas, implementadas por TIC como responsable, como la modificación del protocolo interno de Twitter Group (que la AC IE consideró que no era todo lo claro que debería ser) y las medidas de formación del personal tomadas posteriormente por Twitter, Inc.(se impartió formación adicional para destacar la importancia de mencionar al equipo del DPD, —y por lo tanto a TIC como responsable—, en el sistema de tique interno), así como la existencia de estructuras y garantías internas sobre la responsabilidad respecto a las cuestiones relativas a la protección de la información y la existencia de una auditoría externa recurrente del Programa de protección de la información de Twitter, Inc[173]. Aunque las cuestiones que surgieron no se consideraron indicativas de un problema sistémico más amplio[174] y TIC demostró un enfoque en general proactivamente responsable respecto a la seguridad de los datos[175], se consideró que había un grado de responsabilidad de moderado a grave por parte del responsable, como una falta de claridad en el protocolo que se mostró también en su enmienda posterior[176].

157. El **nivel de cooperación** con la autoridad de control se evaluó en línea con el **artículo 83, apartado 2, letra f) del RGPD**, y bajo ningún concepto se consideró como un factor atenuante[177]. La AC IE reconoció que TIC cooperó plenamente pero indicó que se trataba de una obligación y que TIC no fue más allá del cumplimento de su deber[178].

158. En relación con el **artículo 83, apartado 2, letra g) del RGPD** relativa a las **categorías de datos personales afectados**, el Proyecto de decisión llegó a la conclusión de que cualquier categoría de datos personales se podría haber visto afectada por el retraso en la notificación, y que no se podía decir con toda seguridad que no hubo daños a los interesados o que determinadas categorías de datos personales no se vieron afectadas[179].

159. El **modo en que se comunicó la infracción** a la AC IE se consideró un factor relevante al determinar el importe de la multa (en línea con el artículo 83, apartado 2, letra h) del RGPD), dado que aunque TIC mostró su disposición a presentar toda la documentación disponible, los registros no permitieron a la AC IE verificar el cumplimiento del artículo 33 del RGPD, y la información proporcionada en un principio con la notificación presentada a la AC IE era de naturaleza imprecisa[180].

160. Los criterios del **artículo 83, apartado 2, letras e), i) i j), del RGPD** no se consideraron aplicables, y no se identificaron otros elementos en relación con el **artículo 83, apartado 2, letra k) del RGPD**[181].

161. La AC IE destacó en su Proyecto de decisión que en ausencia de unas directrices específicas a escala de la UE para el cálculo de multas, no estaba obligada a seguir ninguna metodología en particular ni a usar

[172] Proyecto de decisión, apartados 14.39-14.42.
[173] Proyecto de decisión, apartados 14.43-14.47.
[174] Proyecto de decisión, apartado 14.45.
[175] Proyecto de decisión, apartado 14.47.
[176] Proyecto de decisión, apartado 14.47.
[177] Proyecto de decisión, apartado 14.50.
[178] Proyecto de decisión, apartado 14.49.
[179] Proyecto de decisión, apartado 14.54.
[180] Proyecto de decisión, apartado 14.58.
[181] Proyecto de decisión, apartados 14.48, 14.59, 14.60, 14.61.

un punto de partida fijo[182], y que la expresión «tener debidamente en cuenta» proporciona a las AC una amplia discreción sobre cómo valorar los factores del artículo 83, apartado 2, del RGPD[183].

162. En cuanto a la identificación de la correspondiente tarea de calcular el tope máximo de la multa que establece el **artículo 83, apartado 4, del RGPD**, la AC IE destaca que el hecho de que TIC goce de autonomía en su control del tratamiento de datos no significa que deje de ser parte de una **única entidad económica** con su empresa matriz, y observa que, además de que TIC es propiedad de Twitter, Inc., parece ser que el asesor jurídico de Twitter, Inc., es uno de los tres consejeros de TIC[184].

163. Por estos motivos, la ACP calculó el tope máximo para la multa impuesta tomando como referencia el volumen de negocio de Twitter, Inc.[185] Dado que el volumen de negocio de Twitter, Inc., en 2018, ascendió a 3000 millones de USD, se consideró que el tope máximo era de 60 millones de USD (2 % de 3000 millones de USD)[186].

164. Al aplicar los principios de **efectividad, proporcionalidad y capacidad de disuasión** (**artículo 83, apartado 1, del RGPD**), en el Proyecto de decisión se consideró que una multa no puede ser efectiva si no tiene una importancia relativa en los ingresos del responsable del tratamiento, que la infracción no debe considerarse en abstracto, independientemente del impacto en el responsable, y que debe tener capacidad para disuadir de infracciones futuras[187].

165. La AC IE propuso imponer una multa administrativa que oscilara entre 150 000 y 300 000 USD, es decir, entre un 0,005 % y un 0,01 % del volumen de negocio anual de la empresa, i entre un 0,25 % y un 0,5 % del importe máximo de la multa que se podría aplicar por infracciones equivalentes. Lo que, en euros, equivale a una multa de entre 135 000 y 275 000 euros[188].

8.2 Resumen de las objeciones formuladas por las ACI

166. La **AC AT** formuló una objeción sobre el importe de la multa propuesta y el hecho de que la ACP propusiera una gama de importes en vez de un importe fijo. En relación con el artículo 83, apartado 2, letra a) del RGPD, la AC AT destaca que al menos 88 726 personas (aunque probablemente más) se vieron afectadas por la violación de la seguridad y que «*es muy probable que se revelaran datos sensibles al público en general*».

167. La objeción formulada por la AC AT expresa un desacuerdo respecto a cómo se analiza en el Proyecto de decisión el *momento en que debe considerarse que el responsable tuvo conocimiento de una violación de los datos*. Más específicamente, la AC AT argumenta en su objeción que TIC tenía que haber notificado la violación de los datos en un plazo de 72 horas después de que el encargado recibiera el informe del defecto y, por lo tanto, tuviera constancia de la violación. La AC AT destaca que TIC es responsable de supervisar las operaciones de tratamiento efectuadas por su encargado, y que

[182] Proyecto de decisión, apartado 15.2.
[183] Proyecto de decisión, apartado 15.1.
[184] Proyecto de decisión, apartado 15.13.
[185] Proyecto de decisión, apartado 15.14.
[186] Proyecto de decisión, apartado 15.19.
[187] Proyecto de decisión, apartado 15.18.
[188] Proyecto de decisión, apartado 15.20 (el tope máximo de la gama propuesta en el Proyecto de decisión es inferior que en el Proyecto de decisión preliminar con el fin de reflejar los cambios de opinión en relación con la gravedad, el grado de responsabilidad del responsable, y si las infracciones eran sistémicas o no). En el apartado 15.21 del Proyecto de decisión se destaca que, con el fin de proteger los derechos procesales de TIC, se había propuesto una gama de importes para la multa en contraposición a una cifra fija, y se reconoce la posibilidad de que las ACI comenten sobre en qué parte de la gama debe situarse la sanción.

un responsable no debe intentar ocultar el fallo de su encargado con el que tiene una relación contractual y que ha sido seleccionado por el propio responsable. Esto contribuye a evaluar la infracción del artículo 33, apartado 1, del RGPD por parte de la AC AT como «grave».

168. En relación con la «*intencionalidad o negligencia de la infracción*» (artículo 83, apartado 2, letra b), del RGPD), la AC AT argumenta que la conducta de TIC debería etiquetarse como «intencionada» en base a los criterios de conocimiento y voluntad establecidos en las Directrices sobre la aplicación y la fijación de multas administrativas (WP253) del Grupo de trabajo del artículo 29, ratificadas por el CEPD[189]. En cuanto al criterio relativo a las *medidas tomadas para paliar los daños y perjuicios* sufridos por los interesados (artículo 83, apartado 2, letra c) del RGPD), la AC AT destaca que «*inicialmente no era intención de TIC notificar a los usuarios afectados por la violación*» y «*las medidas tomadas por Twitter Inc. para rectificar el defecto son el único factor atenuante*». Finalmente, la AC AT considera que la gama de importes propuesta por la AC IE no es ni efectiva ni proporcionada ni disuasoria en relación con los criterios mencionados en el artículo 83, apartado 2, letras a) a k) del RGPD. En resumen, la AC AT propone la imposición de una multa administrativa más elevada, que sea efectiva, proporcional y disuasoria (en definitiva «*como mínimo que corresponda a un 1 % del volumen de negocios anual de la empresa*»).

169. La **AC DE** formuló una objeción argumentando que la multa propuesta por la ACP es «demasiado baja» y «no cumple las disposiciones del artículo 83, apartado 1, del RGPD». Más específicamente, la AC DE argumenta que la multa no es disuasoria. En la objeción se recuerda que una sanción se puede considerar efectiva y disuasoria si es adecuada como medida preventiva general para disuadir al público en general de cometer infracciones y reafirmar la confianza de la población en la validez del Derecho de la Unión, y también como medida preventiva especial para disuadir al infractor de cometer nuevas infracciones. La AC DE sigue argumentando que la capacidad financiera de una empresa (en términos de volumen de negocio) puede constituir un indicio importante de las cantidades necesarias para alcanzar la disuasión: y ello puede implicar tener en cuenta la parte del volumen de negocio generada por los productos respecto a los cuales se ha cometido la infracción, lo que puede constituir también un indicio de la escala de las infracciones. La AC DE destaca, asimismo, que el efecto disuasorio de las multas elevadas solo se puede alcanzar si los importes impuestos no se pueden pagar fácilmente debido a que se trata de activos grandes o rentas elevadas, y afirma que la multa debe tener un efecto disuasorio, sobre todo, en relación con el tratamiento de datos específicos. En consecuencia, la multa propuesta debe ser suficientemente elevada como para que el tratamiento de datos no sea rentable ni objetivamente eficiente. Dado que el modelo de negocio de Twitter se basa en el tratamiento de datos, y Twitter genera su volumen de negocio básicamente a partir del tratamiento de datos, la AC DE considera que una multa disuasoria en este asunto específico tendría que ser suficientemente elevada como para conseguir que el tratamiento ilegal de datos no sea rentable. En base al concepto de multa aplicable para la AC DE, la multa por la infracción descrita en el Proyecto de decisión debería oscilar entre aproximadamente 7 348 035,00 EUR y 22 044 105,00 EUR.

170. La **AC HU** argumenta que, aunque «*las multas están justificadas cuando se han cometido infracciones*», «*la multa establecida en el Proyecto de decisión no es razonable ni proporcionada, y por lo tanto no es disuasoria teniendo en cuenta la gravedad de la infracción cometida y el poder comercial del responsable del tratamiento a nivel mundial*».

171. La **AC IT** pide a la ACP que «*revise el Proyecto de decisión en relación con la cuantificación de la multa administrativa, teniendo en cuenta también los elementos agravantes específicos del asunto por la*

[189] https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237.

naturaleza del responsable del tratamiento de los datos y la gravedad y la duración de la violación de la seguridad».

8.3 Posición de la ACP respecto a las objeciones

172. La AC IE considera que las objeciones formuladas por la AC AT, la AC DE y la AC HU relativas a la multa administrativa son «pertinentes y motivadas» en el sentido del artículo 4, apartado 24, del RGPD. Al mismo tiempo, la AC IE no ha seguido esas objeciones por los motivos expuestos en el Memorando colectivo[190].

173. En particular, en lo que se refiere a las objeciones de las AC AT y DE, la AC IE considera que su evaluación y aplicación de los factores mencionados en los artículos 83, apartado 2, letras a) y b) del RGPD son adecuadas, como se explica en el Proyecto de decisión. En cuanto a la objeción de la AC AT, la AC IE argumenta que la infracción del artículo 33, apartados 1 y 5, del RGPD por parte de TIC fue el resultado de una negligencia y no de una omisión intencionada[191]. Por lo tanto, la AC IE considera que la multa que propone la AC AT no es proporcionada[192]. Asimismo, la AC IE argumenta que la preocupación de la AC AT en relación con la gama de importes de la multa que se propone en el Proyecto de decisión en contraposición a una suma fija no está bien explicada ni suficientemente clara por parte de esta ACI[193]. En cuanto a la objeción de la AC DE, la AC IE toma nota de la objeción de la AC DE en relación con la necesidad de que la multa debe cumplir el criterio de disuasión, pero opina que el nivel de la multa propuesta por la AC DE no es proporcionado en este caso[194]. Por las razones mencionadas, la AC IE considera que estas objeciones son motivadas y pertinentes, pero propone no seguirlas[195].

174. LA AC IE ha tenido en cuenta debidamente la opinión de la AC AT en relación con los plazos de información y notificación de la violación de la seguridad, pero llega a la conclusión de que, independientemente de que en realidad TIC tuviera conocimiento de la violación el 7 de enero de 2019, TIC debería haber tenido conocimiento de la misma como muy tarde el 3 de enero de 2019[196]. [197] Al identificar el 3 de enero de 2019 como la fecha en la que TIC debería haber tenido conocimiento de la violación de la seguridad, la AC IE también tuvo en cuenta que había habido un retraso anterior durante el período transcurrido entre el momento en que el incidente fue notificado por el contratista a Twitter, Inc. y cuándo Twitter, Inc. empezó su revisión. Asimismo, la AC IE aclara que no sugiere que «*en general los responsables del tratamiento de datos tengan que tener automáticamente conocimiento de las violaciones de la seguridad en el mismo momento que adquiere ese conocimiento el encargado del tratamiento*»[198]. Además, la AC IE indica que «*lo habitual es que un encargado que experimente una violación de la seguridad tenga conocimiento del incidente antes que el responsable, y que, siempre que se siga el procedimiento acordado entre el responsable y el encargado, y sea*

[190] Memorando colectivo, apartados 5.60-5.72.
[191] Memorando colectivo, apartado 5.62.
[192] Memorando colectivo, apartado 5.63.
[193] Memorando colectivo, apartado 5.64.
[194] Memorando colectivo, apartado 5.68.
[195] Memorando colectivo, apartados 5.65, 5.68.
[196] Memorando colectivo, apartado 5.48.
[197] Memorando colectivo, apartado 5.50.
[198] Memorando colectivo, apartado 5.50.

efectivo, el responsable tendrá conocimiento de la violación de la seguridad [...] de tal manera que pueda cumplir su obligación de notificarla»[199].

8.4 Análisis del CEPD

8.4.1 Evaluación de si las objeciones son pertinentes y motivadas

175. En cuanto a la posibilidad de que las objeciones pertinentes y motivadas respecto a si la actuación prevista en relación con el responsable o el encargado cumple el RGPD[200] cuestionen el importe de las multas propuestas, el CEPD ha aclarado recientemente que «*es posible que la objeción cuestione los elementos en que se haya basado el cálculo del importe de la multa*»[201]. Este puede ser un ejemplo de objeción relativa a si la actuación propuesta en relación con el responsable o el encargado del tratamiento cumple el RGPD.

176. En el asunto en cuestión, la objeción de la **AC AT** cuestiona los elementos en que se basa la AC IE al calcular el importe de la multa y, por lo tanto, se refiere a la conformidad con el RGPD de la actuación propuesta respecto al responsable del tratamiento. La AC AT aclara la relación entre su objeción y el Proyecto de decisión y demuestra que los cambios propuestos comportarían una conclusión diferente. Además, aporta argumentos sobre por qué se propone la enmienda de la decisión, ofreciendo una interpretación alternativa de tres de los criterios mencionados en el artículo 83 del RGPD y haciendo referencia a argumentos de hecho y de Derecho. La AC AT demuestra claramente la importancia de los riesgos que entraña el Proyecto de decisión, en primer lugar, argumentando que la multa propuesta no es efectiva ni disuasoria, y recordando que, con este fin, se requiere que pueda disuadir al público en general de cometer infracciones similares y reafirmar la confianza de la población en la aplicación del Derecho de la Unión, además de disuadir al responsable de cometer nuevas infracciones. Asimismo, en la evaluación de la gravedad de la infracción, la objeción se refiere también a la medida en que los interesados (más de los que se identificaron en un principio) se vieron afectados por la Violación de la seguridad (p. ej., porque sus tuiteos antes protegidos, y que probablemente incluían datos sensibles, se vieron expuestos al público en general). La presunta intencionalidad de la infracción, conforme a la AC AT, implica un impacto mucho mayor en la capacidad de reconocer lo bueno de lo malo que si se tratara de una infracción por negligencia. A la luz del análisis efectuado, el CEPD considera que la objeción de la AC AT es pertinente y razonada conforme al artículo 4, apartado 24 del RGPD. En consecuencia, el CEPD evaluará el fondo de las cuestiones sustanciales planteadas en esta objeción (véase apartado 8.4.2 más adelante).

177. La objeción de la **AC DE** también se considera pertinente porque se refiere al cumplimiento de la actuación prevista en el RGPD al cuestionar los elementos en los que se basa el cálculo del importe de la multa. Más específicamente, argumenta que la multa impuesta por la AC IE no es disuasoria, y por eso el cálculo realizado no cumple lo dispuesto en el artículo 83, apartado 1, del RGPD. La AC DE aclara que la sanción debe considerarse efectiva y disuasoria cuando sirve como medida preventiva general para disuadir al público en general de cometer infracciones, así como para confirmar la confianza en la validez del Derecho de la Unión, pero también cuando disuade a quien ha cometido el delito de volver a cometer infracciones adicionales. Además, la AC DE demuestra claramente la importancia de los riesgos que el Proyecto de decisión entraña para los derechos y libertades de los interesados

[199] Memorando colectivo, apartado 5.50.
[200] RGPD, artículo 4, apartado 24.
[201] Directrices sobre OPM, apartado 34.

porque es posible que el hecho de no imponer una sanción disuasoria y efectiva no permita impedir que el responsable del tratamiento cometa nuevas infracciones.

178. Otro argumento proporcionado por la AC DE para demostrar la importancia de los riesgos es que el hecho de no gestionar adecuadamente la infracción sugiere la existencia de un «*error sistémico*», que habría obligado a someter al responsable del tratamiento a un escrutinio más profundo, más allá de este incidente único específico. La AC DE también recuerda que un gran número de personas se vio afectado, y el período de tiempo también fue considerable, y llega a la conclusión de que el poder correctivo impuesto conforme al artículo 58, apartado 2, del RGPD, debe examinarse a la luz de esos elementos. Para finalizar, el CEPD considera que la objeción de la AC DE es motivada y pertinente conforme a la definición del artículo 4, apartado 24, del RGPD. En consecuencia, el CEPD evaluará el fondo de las cuestiones sustanciales planteadas en esta objeción (véase apartado 8.4.2 más adelante).

179. La objeción de la **AC HU** es relevante porque también se refiere al cumplimiento de la actuación prevista en el RGPD, al afirmar que la multa propuesta es «*injustificadamente baja, desproporcionada y no disuasoria*». No obstante, aunque la objeción se refiere al «*"defecto" de la aplicación del responsable a lo largo de los años» y a «su gravedad que afecta a la seguridad de los datos*», así como a «*la gravedad de la infracción cometida*» y al «*poder comercial mundial del responsable del tratamiento*», no demuestra claramente la importancia de los riesgos que el importe de la multa que propone la AC IE entraña para los derechos y libertades de los interesados. En consecuencia, el CEPD considera que esta objeción no cumple los requisitos del artículo 4, apartado 24, del RGPD[202].

180. Finalmente, también queda demostrada la pertinencia de la objeción planteada por la **AC IT** con su referencia a si la actuación propuesta cumple el RGPD, dado que argumenta que la AC IE debería revisar el Proyecto de decisión en relación con la cuantificación de la multa administrativa. Al hacer referencia a las «*objeciones anteriores*» y por lo tanto al hecho de que los aspectos mencionados son «*estructurales por su naturaleza en relación con la organización del responsable*» y «*sujetos a producir efectos no simplemente sobre el asunto en cuestión, sino también sobre cualquier otra violación de datos que pueda ocurrir en el futuro*», la objeción de la AC IT demuestra claramente la importancia de los riesgos para los derechos y libertades de los interesados en relación con la cuantificación de la multa.

181. Por lo tanto, el CEPD considera que la objeción de la AC IT es motivada y pertinente conforme a la definición del artículo 4, apartado 24, del RGPD. En consecuencia, el CEPD evaluará el fondo de las cuestiones sustanciales planteadas en esta objeción.

8.4.2 Evaluación del fondo de las cuestiones sustanciales planteadas en las objeciones pertinentes y motivadas

182. El CEPE considera que las objeciones que se han considerado pertinentes y motivadas en este subapartado[203] requieren la evaluación de si el Proyecto de decisión propone una multa conforme con los criterios establecidos por el artículo 83 del RGPD y las Directrices del grupo de trabajo del artículo

[202] En consecuencia, el CEPD no se pronuncia sobre el fondo de ninguna cuestión sustancial planteada en dichas objeciones. El CEPD reitera que su decisión actual es sin perjuicio de posibles evaluaciones que se puedan requerir del CEPD en otros asuntos, incluso con las mismas partes, teniendo en cuenta el contenido del Proyecto de decisión en cuestión y las objeciones formuladas por las ACI.
[203] Se trata de las objeciones de la AC AT, AC DE y AC IT.

29 sobre la aplicación y la fijación de multas administrativas a efectos del Reglamento 2016/679 (WP253) (ratificadas por el CEPD)[204].

183. De hecho, también se puede usar el mecanismo de coherencia para promover una aplicación coherente de las multas administrativas[205]: cuando una objeción pertinente y motivada cuestiona los elementos en que se basó la ACP para calcular el importe de la multa, el CEPD puede dar instrucciones a la ACP para que inicie un nuevo cálculo de la multa propuesta eliminando las deficiencias en el establecimiento de vínculos causales entre los hechos en cuestión y la forma cómo se calculó la multa propuesta en base a los criterios del artículo 83 del RGPD y los estándares comunes establecidos por el CEPD[206]. Una multa debe ser eficiente, proporcionada y disuasoria, como requiere el artículo 83, apartado 1, del RGPD teniendo en cuenta los hechos del asunto[207]. Además, al decidir el importe de la multa, la ACP debe tener en cuenta los criterios enumerados en el artículo 83, apartado 2, del RGPD.

184. En cuanto a la naturaleza, la gravedad y la duración de la infracción conforme al artículo 33, apartados 1 y 5 del RGPD, el **artículo 83, apartado 2, letra a) del RGPD** obliga a tener en cuenta, entre otras cosas, **la naturaleza, el alcance y la finalidad del tratamiento en cuestión** así como el **número de interesados afectados** y la **gravedad del daño** sufrido por ellos.

185. El CEPD está de acuerdo con la AC IE en que la infracción que se considera no es la violación como tal sino el cumplimiento del artículo 33, apartados 1 y 5, del RGPD al notificar la violación a la AC competente y documentar la Violación.

186. El CEPD observa que la AC IE tiene en cuenta la naturaleza del tratamiento, así como el número de interesados afectados. En cuanto a la **naturaleza del tratamiento**, la AC IE la describe como «microblogging» y plataforma de redes sociales en la que los usuarios pueden expresar sus pensamientos en forma de tuiteos o «tweets». El CEPD considera que, al evaluar la naturaleza del tratamiento, debe tenerse en cuenta también el hecho de que la «operación de tratamiento de que se trate» se refería a comunicaciones de los interesados que deliberadamente eligieron restringir los destinatarios de dichas comunicaciones. El CEPD observa que en el Proyecto de decisión de la AC IE se considera que: «*el impacto en los usuarios individuales, y la posibilidad de que surjan daños de todo ello, dependerá del nivel de datos personales hechos públicos y, también, de la naturaleza de dichos datos personales. En este sentido, ya indiqué en el Proyecto preliminar que, aunque TIC no había confirmado la naturaleza precisa de los datos hechos públicos debido a la violación de la seguridad, era razonable deducir que, dada la escala de los usuarios afectados y la naturaleza del servicio ofrecido por TIC, algunos de los datos personales publicados en relación con, al menos, algunos de los usuarios pertenecían a categorías de datos sensibles y otro material especialmente privado*»[208]. Sin embargo, la AC IE, basándose en las respuestas de TIC, otorgó ahora menos peso a este factor que en el Proyecto de decisión preliminar, dado que no había pruebas directas de daños[209]. No obstante, el CEPD considera que la AC IE debería haber seguido otorgando más peso al hecho de que «la operación de tratamiento de que se trate» implica comunicaciones de interesados que deliberadamente eligieron restringir a los destinatarios de dichas comunicaciones, al evaluar la naturaleza del tratamiento en

[204] Directrices del grupo de trabajo del artículo 29 sobre la aplicación y la fijación de multas administrativas a efectos del Reglamento 2016/679, WP253, aprobadas el 3 de octubre de 2017 (ratificadas por el CEPD el 25 de mayo de 2020).
[205] Considerando 150 del RGPD.
[206] Directrices sobre OPM, apartado 34.
[207] Directrices del CEPD sobre multas administrativas, pág. 7.
[208] Proyecto de decisión, apartado 14.51.
[209] Ver apartado 150 anterior.

cuestión. En particular, la AC IE debería haber otorgado un peso significativo a este hecho dado que ella misma lo recuerda en el Proyecto de decisión, donde considera que «*la gran escala del segmento de usuarios afectados da lugar a la posibilidad de un espectro mucho más amplio de daños derivados de la violación de la seguridad, especialmente dada la naturaleza del servicio ofrecido por TIC*» y «*la probabilidad de que muchos usuarios habrán confiado en la función de conservar la privacidad de los tuiteos para compartir información u opiniones (dado que consideraban que era un entorno privado y controlado) que no habrían publicado en un entorno de dominio público*»[210].

187. Además, cuando se trata del alcance del tratamiento en cuestión, parece que la AC IE sustituye el alcance del tratamiento por el número de interesados afectados. El CEPD considera que **la naturaleza y el alcance del «tratamiento»** que hay que tener en cuenta en la determinación de la multa no es la operación de tratamiento que consiste en la revelación (accidental) (violación de la seguridad de datos personales), o la causa de la misma, sino el alcance del tratamiento subyacente realizado por TIC, como se describe en el apartado anterior.

188. Según la AC AT, **el momento en que el responsable fue consciente de la violación de la seguridad influye en la gravedad de la infracción** del artículo 33, apartado 1) del RGPD. La objeción formulada por la AC AT expresa un desacuerdo respecto a cómo se debe determinar y analizar el momento en que debe considerarse que el responsable tuvo conocimiento de una violación de los datos. Más específicamente, la AC AT argumenta en su objeción que TIC tenía que haber notificado la violación de los datos en un plazo de 72 horas después de tener conocimiento del defecto. Esto contribuye a evaluar la infracción del artículo 33, apartado 1, del RGPD por parte de la AC AT como «grave».

189. En este sentido, el CEPD recuerda que las Directrices sobre notificación de las violaciones de datos personales de acuerdo con el Reglamento 2016/679 («WP250»)[211], ratificadas por el CEPD, establecen que «*cualquier plan de respuesta en caso de violación debe centrarse en la protección de las personas y de sus datos personales. Por consiguiente, la notificación de las violaciones de la seguridad debe considerarse como una herramienta que mejora el cumplimiento respecto de la protección de los datos personales*»[212].

190. Según las Directrices sobre la notificación de las violaciones de la seguridad de los datos personales, debe considerarse que un responsable del tratamiento «tiene constancia» cuando tenga un grado razonable de certeza de que se ha producido un suceso que compromete datos personales[213]. Dado que el responsable del tratamiento utiliza al encargado para este fin, en principio debe considerarse que el responsable «tiene constancia» cuando el encargado le informa de la violación de la seguridad[214]. Sin embargo, el RGPD impone al responsable la obligación de garantizar que tendrá constancia de las violaciones de forma puntual, para poder llevar a cabo la actuación adecuada[215] y explica que «*el responsable del tratamiento podrá iniciar un breve período de investigación para determinar si se ha producido o no una violación. Durante este período de investigación, no se puede*

[210] Proyecto de decisión, apartado 14.51.

[211] Artículo 29 Directrices sobre la notificación de las violaciones de la seguridad de los datos personales de acuerdo con el Reglamento 2016/679, WP250 rev.01, ratificadas por el CEPD (en adelante las «Directrices sobre notificación de violaciones de la seguridad de los datos personales»).

[212]Directrices sobre notificación de violaciones de la seguridad de los datos personales, pág. 5.

[213] Directrices sobre notificación de violaciones de la seguridad de los datos personales, pág. 10-11.

[214] Directrices sobre notificación de violaciones de la seguridad de los datos personales, pág. 13.

[215] Directrices sobre notificación de violaciones de la seguridad de los datos personales, pág. 11.

considerar que el responsable del tratamiento "tenga constancia".»[216]. Sin embargo, las Directrices dejan claro que esta investigación inicial debe empezar tan pronto como sea posible y que más adelante se puede llevar a cabo una investigación más detallada[217].

191. De este modo las Directrices dejan claro que el responsable, y por extensión el encargado, deben actuar con celeridad. «En la mayoría de los casos, estas acciones preliminares deben realizarse poco después de la alerta inicial (es decir, *cuando el responsable o el encargado del tratamiento sospeche que se ha producido un incidente de seguridad que pueda afectar a datos personales*) —solo en casos excepcionales debe tardarse más tiempo»[218].

192. Teniendo en cuenta todo esto, el CEPD está de acuerdo con la postura de la evaluación de la AC IE según la cual no se puede esperar que el responsable tenga constancia del hecho en el mismo momento en que el encargado se da cuenta de que ha habido un incidente de seguridad. Como se indica en las Directrices del grupo de trabajo 29 sobre notificación de las violaciones de la seguridad, ratificadas por el CEPD, tiene que haber un grado de certeza de que ha habido una violación de la seguridad de los datos personales antes de que se pueda estipular la constancia. De los hechos en cuestión que se reflejan en el Proyecto de decisión no queda claro si este fue el caso antes del 3 de enero de 2019. En este asunto, la AC AT no demuestra que TIC tuviera el grado necesario de certeza respecto a que se hubiera producido una violación de la seguridad de los datos personales antes de la fecha en que la AC IE consideró que TIC «tenía constancia» de la violación. En consecuencia, el CEPD considera que la evaluación de la gravedad de la infracción no debe adaptarse a la luz de una determinación diferente de cuando el responsable tuvo conocimiento de la violación de la seguridad.

193. Asimismo, en cuanto a **la gravedad de la infracción**, el CEPD está de acuerdo con la AC IE en que el cumplimiento de los artículos 33, apartados 1 y 5, del RGPD es esencial para el funcionamiento global del régimen de supervisión y ejecución.

194. En cuanto a la objeción planteada por la AC AT sobre la **naturaleza intencionada de la infracción**, el CEPD considera que la objeción no demuestra suficientemente que, a partir del momento en que el responsable tuvo conocimiento de la violación, hubiera eludido intencionadamente su obligación de actuar.

195. Sin embargo, en lo que se refiere a la naturaleza negligente de la infracción, el CEPD considera que una empresa para la cual el tratamiento de datos personales es la esencia de sus actividades debe tener implantado un procedimiento suficiente para la documentación de violaciones de la seguridad de los datos personales, con medidas correctivas, que permitan también cumplir la obligación de notificación conforme al artículo 33, apartado 1, del RGPD. Este elemento implica un elemento adicional a tener en cuenta en el análisis de la gravedad de la infracción.

196. El CEPD recuerda que el TJUE ha sostenido reiteradamente que una sanción disuasoria es una sanción que tiene un **auténtico efecto disuasorio**[219]. En este sentido, se puede distinguir entre disuasión general (que disuade a otros de cometer la misma infracción en el futuro) y disuasión específica (que

[216] Directrices sobre notificación de violaciones de la seguridad de los datos personales, pág. 11 (subrayado añadido).
[217] Directrices sobre notificación de violaciones de la seguridad de los datos personales, pág. 11.
[218] Directrices sobre notificación de violaciones de la seguridad de los datos personales, pág. 12 (cursiva añadida).
[219] Véase el dictamen del Abogado General Geelhoed de 29 de abril de 2004 en la sentencia de 12 de julio de 2005, Comisión / Francia, C-304/02, EU:C:2005:444, ap. 39.

desalienta al destinatario de la multa de cometer de nuevo la misma infracción)[220]. Además, la gravedad de las sanciones debe ser proporcional a la gravedad de las infracciones por las que se imponen[221]. De ello se deduce que las multas no deben ser desproporcionadas respecto a los fines perseguidos, es decir, el cumplimiento de las reglas de protección de datos, y que el importe de la multa impuesta a una empresa debe ser proporcional a la infracción vista en conjunto, teniendo en cuenta en particular la gravedad de la infracción[222].

197. Aunque la ACP en su Proyecto de decisión hacía referencia al requisito de que la multa debía ser **disuasoria y proporcionada**, el CEPD considera que la ACP no ha argumentado suficientemente cómo podría satisfacer esos requisitos la multa propuesta. En particular, el CEPD observa que la ACP pasa de calcular el importe máximo de la multa (establecido en 60 millones de euros) a establecer una gama de importes (entre 150 000,00 y 300 000,00 dólares estadounidenses), sin más explicación respecto a qué elementos concretos llevaron a la ACP a identificar esta gama concreta[223]. Más allá de la referencia general a los factores pertinentes del artículo 83, apartado 2, del RGPD, no existe una motivación clara de por qué se ha elegido el porcentaje propuesto (entre un 0,25 % y un 0,5 %) del máximo aplicable según el artículo 83, apartado 4, del RGPD.

198. En este sentido, el CEPD ha explicado más arriba los motivos por los que la ACP, en su Proyecto de decisión, debería haber otorgado más peso al elemento relativo a la naturaleza, el alcance y la negligencia de la infracción, y, por lo tanto, considera que la gama de importes propuesta debería adaptarse en consecuencia.

8.4.3 Conclusión

199. Por lo tanto, el CEPD considera que la multa propuesta en el Proyecto de decisión es demasiado baja y no cumple su finalidad como medida correctiva, en particular no satisface los requisitos del artículo 83, apartado 1, del RGPD, de ser eficiente, disuasoria y proporcional.

200. Así pues, el CEPD solicita a la AC IE que vuelva a evaluar los elementos en que se basa para calcular el importe de la multa fija[224] que debe imponerse a TIC, para garantizar que sea adecuada para este asunto.

201. El CEPD observa que el análisis de las objeciones se limita al contenido de las objeciones que se consideran motivadas y pertinentes. El alcance del análisis del CEPD sobre el cálculo de la multa se limita, pues, a un análisis del método de cálculo de las multas como tales. No constituye una validación implícita o explícita por parte del CEPD del análisis efectuado por la ACP en cuanto a la infracción del artículo 33, apartados 1 y 5, del RGPD, o la cualificación jurídica de Twitter Inc. y TIC respectivamente. El CEPD reitera que su decisión actual se entiende sin perjuicio de posibles evaluaciones que se puedan requerir del CEPD en otros asuntos, incluso con las mismas partes, teniendo en cuenta el contenido del Proyecto de decisión en cuestión y las objeciones formuladas por las ACI.

[220] Véase también, entre otras, la sentencia de 13 de junio de 2013, Versalis Spa / Comisión, C-511/11, ECLI: EU:T:2013:386, ap. 94.
[221] Sentencia del TJUE del 25 de abril de 2013, Asociaţia Accept, C-81/12.
[222] Marine - Harvest EU General Court T-704/14, 26 de octubre de 2017.
[223] Proyecto de decisión 15.19 y 15.20.
[224] Preferiblemente, debería haberse incluido en el proyecto de decisión del artículo 60 del RGPD.

9 DECISIÓN VINCULANTE

202. A la luz de lo anterior, y de acuerdo con la función del CEPD, en virtud del artículo 70, apartado 1, letra t) del RGPD, de emitir decisiones vinculantes con arreglo al artículo 65 del RGPD, el Comité emite la siguiente decisión vinculante de acuerdo con el artículo 65, apartado 1, letra a) del RGPD:

203. Acerca de las objeciones relativas a la cualificación de responsable y encargado del tratamiento y la competencia de la ACP:

- El CEPD decide que la AC IE no está obligada a modificar su Proyecto de decisión en base a las objeciones formuladas, dado que no cumplen los requisitos contemplados en el artículo 4, apartado 24, del RGPD.

204. Acerca de las objeciones relativas a las infracciones del artículo 33, apartados 1 y 5 del RGPD detectadas por la ACP:

- En relación con la objeción de la AC FR sobre la ausencia de una infracción del artículo 33, apartado 1, del RGPD, la objeción de la AC DE sobre la determinación del *dies a quo* para la infracción del artículo 33, apartado 1, del RGPD, y la objeción de la AC IT relativa a la infracción del artículo 33, apartado 5, del RGPD, el CEPD decide que la AC IE no debe modificar su Proyecto de decisión en base a las objeciones formuladas, porque no satisfacen los requisitos del artículo 4, apartado 24, del RGPD.

205. Acerca de las objeciones relativas a posibles infracciones adicionales (o alternativas) del RGPD identificadas por las ACI:

- En relación con la objeción de la AC DE sobre posibles infracciones del artículo 5, apartado 1, letra f), el artículo 24 y el artículo 32 del RGPD, y a la objeción de la AC IT sobre la posible infracción del artículo 5, apartado 2, del RGPD, el CEPD decide que, a pesar de que cumplen los requisitos del artículo 4, apartado 24, del RGPD, no es necesario que la AC IE modifique su Proyecto de decisión porque los elementos de hecho disponibles incluidos en el Proyecto de decisión y en las objeciones no son suficientes para que el CEPD pueda establecer la existencia de infracciones del artículo 5, apartado 1, letra f), el artículo 5, apartado 2, el artículo 24 y el artículo 32 del RGPD.

- En relación con la objeción de la AC DE sobre la posible infracción del artículo 33, apartado 3, del RGPD, la objeción de la AC FR sobre la posible infracción del artículo 28 y el artículo 32 del RGPD, la objeción de la AC HU sobre la posible infracción del artículo 5, apartado 1, letra f), el artículo 32 y el artículo 34 del RGPD, y la objeción de la AC IT relativa a la posible infracción del artículo 28 del RGPD, el CEPD decide que la AC IE no debe modificar su Proyecto de decisión en base a las objeciones formuladas, porque no satisfacen los requisitos del artículo 4, apartado 24, del RGPD.

206. Acerca de la objeción sobre la decisión de la ACP de no emitir una sanción con apercibimiento:

- En relación con la objeción de la AC DE sobre la decisión de la AC IE de no emitir una sanción con apercibimiento, el CEPD decide que la AC IE no debe modificar su Proyecto de decisión en base a las objeciones formuladas, dado que no cumplen los requisitos del artículo 4, apartado 24, del RGPD.

207. Acerca de la objeción relativa al cálculo de la multa sugerida por la ACP:

- En relación con la objeción de la AC HU sobre la insuficiente naturaleza disuasoria de la multa, el CEPD decide que la AC IE no debe modificar su Proyecto de decisión en base a la objeción formulada, dado que no cumple los requisitos del artículo 4, apartado 24, del RGPD.
- En relación con la objeción de la AC AT, la objeción de la AC DE y la objeción de la AC IT sobre la insuficiente naturaleza disuasoria de la multa, el CEPD decide que satisfacen los requisitos del artículo 4, apartado 24, del RGPD, y que la AC IE debe valorar de nuevo **los elementos en los que se basa el cálculo del importe de la multa fija** que debe imponerse a TIC, y modificar su Proyecto de decisión aumentando el valor de la multa para asegurar que cumple su finalidad como medida correctiva y satisface los requisitos de eficiencia, disuasión y proporcionalidad establecidos en el artículo 83, apartado 1, del RGPD y teniendo en cuenta los criterios del artículo 83, apartado 2, del RGPD.

10 OBSERVACIONES FINALES

208. Esta decisión vinculante se dirige a la AC IE y a las ACI. La AC IE adoptará su decisión final en base a esta decisión vinculante conforme al artículo 65, apartado 6, del RGPD.

209. En cuanto a las objeciones que se ha considerado que no cumplen los requisitos del artículo 4, apartado 24, del RGPD, el CEPD no se pronuncia sobre el fondo de ninguna cuestión sustancial en dichas objeciones. El CEPD reitera que su decisión actual se entiende sin perjuicio de posibles evaluaciones que se puedan requerir del CEPD en otros asuntos, incluso con las mismas partes, teniendo en cuenta el contenido del Proyecto de decisión en cuestión y las objeciones formuladas por las ACI.

210. En virtud del artículo 65, apartado 6, del RGPD, la AC IE debe comunicar su decisión final a la Presidencia en el plazo de un mes tras recibir la decisión vinculante.

211. Una vez realizada dicha comunicación por la AC IE, la decisión vinculante se hará pública conforme al artículo 65, apartado 5, del RGPD.

212. Con arreglo al artículo 70, apartado 1, letra y) del RGPD, la decisión final de la AC IE comunicada al CEPD se incluirá en el registro de decisiones que hayan sido objeto del mecanismo de coherencia.

Por el Comité Europeo de Protección de Datos

La Presidenta

(Andrea Jelinek)