GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29

844/14/ES
WP 217

Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE

Adoptado el 9 de abril de 2014

Índice

Resumen

En el presente Dictamen se analizan los principios establecidos en el artículo 7 de la Directiva 95/46/CE relativos a la legitimación del tratamiento de datos. Tras analizar, en concreto, el interés legítimo del responsable del tratamiento, se ofrece orientación sobre cómo aplicar el artículo 7, letra f), de conformidad con el marco jurídico actual y se formulan recomendaciones para mejoras futuras.

El artículo 7, letra f), es el último de los seis fundamentos jurídicos del tratamiento de los datos personales. De hecho, este fundamento jurídico requiere una prueba de sopesamiento entre el interés legítimo del responsable del tratamiento o cualesquiera terceros a los que se comuniquen los datos y los intereses o los derechos fundamentales del interesado. El resultado de esta prueba de sopesamiento determinará si el artículo 7, letra f), puede utilizarse como fundamento jurídico del tratamiento.

El Grupo de trabajo del artículo 29 reconoce la importancia y la utilidad del principio del artículo 7, letra f) que, en las circunstancias correctas y sujeto a las garantías adecuadas, puede ayudar a evitar una dependencia excesiva de otros fundamentos jurídicos . El artículo 7, letra f), no deberá utilizarse como «un último recurso» para situaciones raras o inesperadas en las que se considere que no son aplicables otros fundamentos jurídicos del tratamiento. No obstante, no deberá elegirse automáticamente ni deberá extenderse su uso de manera indebida basándose en la percepción de que es menos restrictivo que los demás fundamentos.

Una valoración apropiada del artículo 7, letra f), no es un examen de ponderación directo que consista solamente en sopesar dos «pesos» fácilmente cuantificables y comparables en la balanza. Por el contrario, dicho examen requiere una consideración completa de una serie de factores, con el fin de garantizar que se tienen en cuenta debidamente los intereses y los derechos fundamentales de los afectados. Al mismo tiempo, se trata de una prueba modulable, que puede variar desde sencilla hasta compleja, y no es necesario que resulte indebidamente onerosa. Los factores que deben considerarse cuando se efectúe dicha prueba de sopesamiento comprenderán:

- la naturaleza y la fuente del interés legítimo, y si el tratamiento de datos es necesario para el ejercicio de un derecho fundamental, resulta de otro modo de interés público o se beneficia del reconocimiento de la comunidad afectada;

- la repercusión para el interesado y sus expectativas razonables sobre qué sucederá con sus datos, así como la naturaleza de los datos y la manera en la que sean tramitados;

- las garantías adicionales que podrían limitar un impacto indebido sobre el interesado, tales como la minimización de los datos, las tecnologías de protección de la intimidad, el aumento de la transparencia, el derecho general e incondicional de exclusión voluntaria y la portabilidad de los datos.

De cara al futuro, el Grupo de trabajo del artículo 29 recomienda añadir a la propuesta de Reglamento un considerando sobre los factores clave que deben considerarse al efectuar dicha prueba de sopesamiento. El Grupo de trabajo del artículo 29 también recomienda que se añada un considerando en el que se exija al responsable del tratamiento, cuando proceda, que documente su valoración en aras de una mayor responsabilidad. Por último, el Grupo de trabajo del artículo 29 también apoya una disposición sustantiva relativa a los

responsables del tratamiento con el fin de que estos expliquen a los interesados los motivos por los que creen que sus intereses prevalecerían sobre los derechos fundamentales y las libertades del interesado .

EL GRUPO DE TRABAJO SOBRE LA PROTECCIÓN DE LAS PERSONAS FÍSICAS EN LO QUE RESPECTA AL TRATAMIENTO DE LOS DATOS PERSONALES

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

vistos los artículos 29 y 30, apartado 1, letra a), y apartado 3 de la citada Directiva,

visto su Reglamento interno,

HA ADOPTADO EL PRESENTE DICTAMEN:

I. Introducción

En el presente Dictamen se analizan los principios establecidos en el artículo 7 de la Directiva 95/46/CE[1] (la «Directiva») relativos a la legitimación del tratamiento de datos. Se centra, en particular, en el interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7, letra f).

Los principios enumerados en el artículo 7 están relacionados con el principio más amplio de «licitud» estipulado en el artículo 6, apartado 1, letra a), que exige que los datos personales sean tratados «de manera leal y lícita».

En el artículo 7 se exige que se permita el tratamiento de los datos personales únicamente si es aplicable al menos uno de los seis fundamentos jurídicos enumerados en dicho artículo. En especial, los datos personales solo serán tratados a) basándose en el consentimiento inequívoco del interesado[2]; o si, dicho brevemente[3], el tratamiento es necesario para:

b) la ejecución de un contrato con el interesado;
c) el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento;
d) la protección del interés vital del interesado;
e) el cumplimiento de una misión de interés público; o
f) la satisfacción del interés legítimo perseguido por el responsable del tratamiento, sujeto a un examen de ponderación adicional en relación con los intereses y los derechos del interesado.

Este último fundamento jurídico permite el tratamiento «necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezcan los intereses o[4] los derechos y

---

1 Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DO L 281 de 23.11.1995, p. 31).

2 Véase el Dictamen 15/2011 del Grupo de trabajo sobre protección de datos del artículo 29 sobre la definición del consentimiento, adoptado el 13 de julio de 2011 (WP187).

3 Estas disposiciones se examinan con más detalle posteriormente.

4 Tal como se explica en la sección III.3.2, la versión de la Directiva en lengua inglesa contiene un error tipográfico: el texto debe decir «interests or fundamental rights» en lugar de «interests for fundamental rights».

libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva». En otras palabras, el artículo 7, letra f), permite el tratamiento sujeto a una prueba de sopesamiento que pondere el interés legítimo del responsable del tratamiento, o del tercero o terceros a los que se comuniquen los datos, en relación con los intereses o los derechos fundamentales de los interesados[5].

Necesidad de un enfoque más coherente y armonizado en Europa

Los estudios realizados por la Comisión en el marco de la revisión de la Directiva[6], así como la cooperación y el intercambio de puntos de vista entre las autoridades nacionales de protección de datos, han puesto de manifiesto una carencia de interpretación armonizada del artículo 7, letra f), de la Directiva, que ha dado lugar a aplicaciones divergentes en los Estados miembros. En especial, aunque se exige efectuar una auténtica prueba de sopesamiento en varios Estados miembros, el artículo 7, letra f), se percibe a veces de manera incorrecta como una «puerta abierta» para legitimar cualquier tratamiento de datos que no se justifique con ninguno de los demás fundamentos jurídicos .

La carencia de un enfoque coherente puede dar lugar a una falta de seguridad jurídica y de previsibilidad, puede debilitar la posición de los interesados y puede también imponer cargas reglamentarias innecesarias a las empresas y a otras organizaciones con operaciones transfronterizas. Dichas incoherencias ya han dado lugar a litigios ante el Tribunal de Justicia de la Unión Europea[7] («TJUE»).

Resulta particularmente oportuno, por tanto, mientras prosiguen los trabajos para la elaboración de un nuevo Reglamento general de protección de datos, que el sexto fundamento jurídico del tratamiento (en referencia al «interés legítimo») y su relación con los demás fundamentos jurídicos del tratamiento, se comprenda de manera más clara. En especial, el hecho de que estén en juego los derechos fundamentales de los interesados implica que la aplicación de los seis fundamentos jurídicos en conjunto debería, debida y equitativamente, tener en cuenta el respeto de estos derechos. El artículo 7, letra f), no deberá convertirse en un camino fácil para eludir el cumplimiento de la legislación sobre la protección de datos.

Por este motivo, el Grupo de trabajo del artículo 29 sobre la protección de datos («el Grupo de trabajo»), como parte de su programa de trabajo para 2012-2013, ha decidido examinar

---

5 La referencia al artículo 1, apartado 1, no deberá interpretarse como una limitación del alcance de los intereses y los derechos y libertades fundamentales del interesado. Por el contrario, la función de esta referencia es enfatizar el objetivo global de las leyes de protección de datos y de la propia Directiva. De hecho, el apartado 1 del artículo 1 no solo se refiere a la protección de la privacidad sino también a la protección de todos los demás «derechos y libertades de las personas físicas», siendo la privacidad solo uno de ellos.

6 El 25 de enero de 2012 la Comisión Europea adoptó un paquete de reformas del marco legislativo europeo sobre la protección de datos. Dicho paquete comprende: i) una «Comunicación» (COM(2012)9 final), ii) una propuesta de un «Reglamento general de protección de datos» («propuesta de Reglamento») (COM(2012)11 final) y iii) una propuesta de «Directiva» sobre la protección de datos en el ámbito de la aplicación del Derecho penal (COM(2012)10 final). La «Evaluación de impacto» adjunta, que contiene diez anexos, se recoge en un documento de trabajo de la Comisión (SEC(2012)72 final). Véase, en especial, el estudio titulado «Evaluación de la aplicación de la Directiva de protección de datos», que constituye el anexo 2 de la Evaluación de impacto adjunta al paquete de reformas del marco legislativo sobre la protección de datos de la Comisión Europea.

7 Véase la página 7, bajo el epígrafe «II.1 Breve historia», *«La aplicación de la Directiva; la sentencia de ASNEF y FECEMD»*.

minuciosamente esta cuestión y, con el fin de llevar a cabo dicho programa de trabajo[8], se ha comprometido a elaborar el presente Dictamen.

Aplicación del marco jurídico vigente y preparación del futuro

En el propio programa de trabajo se fijaban claramente dos objetivos: «garantizar la aplicación correcta del marco jurídico vigente» y también «preparar el futuro».

Por consiguiente, el primer objetivo del presente Dictamen es garantizar un entendimiento común del marco jurídico vigente. Este objetivo es la continuación de Dictámenes anteriores sobre otras disposiciones clave de la Directiva[9]. En segundo lugar, partiendo del análisis, este Dictamen también formulará recomendaciones políticas que deberán considerarse durante la revisión del marco jurídico sobre la protección de datos.

Estructura del Dictamen

Después de un breve resumen de la historia y la función del interés legítimo y otros fundamentos del tratamiento en el capítulo II, en el capítulo III se examinarán e interpretarán las disposiciones pertinentes de la Directiva, teniendo en cuenta la motivación común en su aplicación nacional. Este análisis se acompaña de ejemplos prácticos basados en la experiencia nacional, y apoya las recomendaciones del capítulo IV tanto respecto de la aplicación del marco normativo vigente como en el contexto de revisión de la Directiva.

II. Observaciones generales y cuestiones políticas

II.1. Breve historia

Este resumen se centra en la evolución de los conceptos de legalidad y fundamento jurídico del tratamiento, incluido el interés legítimo. En él se explica, en especial, cómo la necesidad de una base jurídica se utilizó en principio como requisito en el contexto de excepciones de los derechos de privacidad, y más tarde se convirtió en un requisito separado en el contexto de la protección de datos.

Convenio Europeo para la Protección de los Derechos Humanos («CEDH»)

El artículo 8 del Convenio europeo para la protección de los derechos humanos, adoptado en 1950, incorpora el derecho a la privacidad, es decir, el respeto de la vida privada y familiar, del hogar y de la correspondencia. Prohíbe cualquier injerencia en el ejercicio del derecho a la privacidad excepto si «está previsto por la ley» y «es necesario en una sociedad democrática» con el fin de satisfacer determinados tipos de interés público imperativo, específicamente enumerados.

---

8 Véase el programa de trabajo 2012-2013 del Grupo de trabajo del artículo 29 sobre la protección de datos adoptado el 1 de febrero de 2012 (WP190).

9 Tales como el Dictamen 3/2013 sobre la limitación de la finalidad, adoptado el 3 de abril de 2013 (WP203), el Dictamen 15/2011 sobre la definición del consentimiento (citado en el pie de página 2), el Dictamen 8/2010 sobre el Derecho aplicable, adoptado el 16 de diciembre de 2010 (WP179) y el Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento», adoptado el 16 de febrero de 2010 (WP169).

El artículo 8 del CEDH se centra en la protección de la vida privada y exige una justificación de cualquier injerencia en la privacidad. Este enfoque se basa en una prohibición general de injerencia en el derecho a la privacidad y permite excepciones solo en condiciones estrictamente definidas. En los casos en los que exista una «injerencia en la privacidad» se exige una base jurídica, así como la especificación de una finalidad legítima como condición previa para evaluar la necesidad de la injerencia. Este enfoque explica que el CEDH no proporcione una lista de posibles fundamentos jurídicos sino que se concentre en la necesidad de un fundamento jurídico y en los criterios que dicha base jurídica debe cumplir.

Convenio nº 108

El Convenio nº 108 del Consejo de Europa[10], abierto a la firma en 1981, introduce la protección de los datos de carácter personal como un concepto separado. La idea subyacente en aquel momento no era que el tratamiento de los datos personales se considerara siempre como una «*injerencia* en la privacidad», sino que con el fin de *proteger* los derechos y las libertades fundamentales de todas las personas, y en particular su derecho a la privacidad, el tratamiento de los datos personales cumpliera siempre determinadas condiciones. El artículo 5, por tanto, establece los principios fundamentales de la legislación sobre la protección de datos, incluido el requisito de que los datos de carácter personal que sean objeto de un tratamiento automatizado: a) se obtendrán y tratarán leal y legítimamente. Sin embargo, el Convenio no proporciona fundamentos detallados para el tratamiento[11].

Directrices de la OCDE[12]

Las Directrices de la OCDE, preparadas paralelamente al Convenio nº 108 y adoptadas en 1980, comparten ideas similares de «licitud», aunque el concepto se expresa de manera diferente. Estas Directrices se actualizaron en 2013, sin cambios sustantivos en el principio de legalidad. El artículo 7 de las Directrices de la OCDE, en particular, establece que deberán establecerse límites a la recopilación de datos personales y dichos datos deberán obtenerse de manera leal y lícita y, cuando así proceda, con el conocimiento o consentimiento del interesado. Aquí el fundamento jurídico del consentimiento se menciona explícitamente como una opción que deberá utilizarse «cuando así proceda». Esto exigirá una valoración de los intereses y los derechos en juego, así como una evaluación de la medida en que el tratamiento resulta intrusivo. En este sentido, el enfoque de la OCDE tiene algunas similitudes con los criterios, mucho más desarrollados, de la Directiva 95/46/CE.

Directiva 95/46/CE

Cuando se adoptó en 1995, la Directiva partía de los instrumentos previos de protección de datos, incluido el Convenio nº 108 y las Directrices de la OCDE. También se tuvo en

---

10 Convenio nº 108 relativo a la protección de las personas físicas en lo que respecta al tratamiento automatizado de datos de carácter personal.

11 El proyecto de texto del Convenio modernizado adoptado por el pleno del comité consultivo de noviembre de 2012 afirma que el tratamiento de los datos podrá realizarse sobre la base del consentimiento del interesado o sobre la base de «algún fundamento legítimo estipulado por ley», de igual modo que la Carta de Derechos fundamentales de la Unión Europea mencionada posteriormente en la página 9.

12 Directrices de la OCDE sobre la protección de la privacidad y los flujos transfronterizos de datos personales, de 11 de julio de 2013.

consideración la experiencia previa relativa a la protección de datos en algunos Estados miembros.

Además del requisito más amplio establecido en su artículo 6, apartado 1, letra a), de que los datos personales deben ser tratados «de manera leal y lícita», la Directiva añadió una serie específica de requisitos adicionales, que no estaban presentes todavía como tales ni en el Convenio nº 108 ni en las Directrices de la OCDE: el tratamiento de los datos personales debe basarse en uno de los seis fundamentos jurídicos especificados en el artículo 7.

Aplicación de la Directiva; la sentencia de ASNEF y FECEMD[13]

La Comisión, en su informe titulado «Evaluación de la aplicación de la Directiva de protección de datos»[14], destaca que la aplicación de las disposiciones de la Directiva en la legislación nacional a veces no ha resultado satisfactoria. En el análisis técnico de la transposición de la Directiva en los Estados miembros[15], la Comisión facilita más detalles sobre la aplicación del artículo 7. En este análisis se explica que, aunque la legislación en la mayoría de los Estados miembros establece seis fundamentos jurídicos en términos relativamente similares a los utilizados en la Directiva, la flexibilidad de estos principios ha dado lugar, de hecho, a aplicaciones divergentes.

Resulta especialmente pertinente en este contexto que en su sentencia de 24 de noviembre de 2011 sobre el asunto *ASNEF y FECEMD*, el TJUE fallara que España no había transpuesto correctamente el artículo 7, letra f), de la Directiva, exigiendo que, en el caso de que no exista consentimiento del interesado, cualesquiera datos pertinentes utilizados figuren en fuentes accesibles al público. La sentencia también falló que el artículo 7, letra f), tiene efecto directo. La sentencia limita el margen de apreciación de los Estados miembros al aplicar el artículo 7, letra f). En especial, no deben sobrepasar la tenue línea entre la aclaración, por un lado, y el establecimiento de requisitos adicionales, por otro, lo que modificaría el alcance del artículo 7, letra f).

La sentencia, al establecer claramente que no les está permitido a los Estados miembros imponer restricciones y exigencias unilaterales adicionales relativas a los fundamentos jurídicos del tratamiento lícito de datos en sus legislaciones nacionales, tiene consecuencias importantes. Los tribunales nacionales y otros organismos pertinentes deben interpretar las disposiciones nacionales a la luz de esta sentencia y, si es necesario, dejar de lado cualesquiera normas y prácticas nacionales que entren en conflicto.

A la luz de esta sentencia, resulta especialmente importante que se llegue a un claro y común entendimiento de la aplicabilidad del artículo 7, letra f), por parte de las autoridades nacionales de protección de datos y otros legisladores europeos. Esto deberá hacerse de manera equilibrada, sin restringir ni ampliar indebidamente al alcance de esta disposición.

La Carta de los Derechos Fundamentales

---

13 Sentencia del TJUE, de 24.11.2011, en los asuntos C-468/10 y C-469/10 (*ASNEF y FECEMD*).

14 Véase el anexo 2 de la Evaluación de impacto del paquete de reformas del marco legislativo sobre la protección de datos de la Comisión, citado en el pie de página 6 anterior.

15 Análisis y estudio de impacto sobre la aplicación de la Directiva CE 95/46 en los Estados miembros. Véase http://ec.europa.eu/justice/policies/privacy/docs/lawreport/consultation/technical-annex_en.pdf

Desde que entró en vigor el Tratado de Lisboa el 1 de diciembre de 2009, la Carta de los Derechos Fundamentales de la Unión Europea («la Carta») goza del «mismo valor jurídico que los Tratados»[16]. La Carta consagra la protección de los datos personales como un derecho fundamental en virtud del artículo 8, que es diferente del respeto de la vida privada y familiar con arreglo al artículo 7. El artículo 8 establece el requisito de un fundamento legítimo para el tratamiento. En particular, dispone que los datos personales deben tratarse «sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley»[17]. Estas disposiciones refuerzan tanto la importancia del principio de legalidad como la necesidad de una base jurídica adecuada para el tratamiento de los datos personales.

La propuesta de Reglamento de protección de datos

En el contexto del proceso de revisión del marco legislativo sobre la protección de datos, el alcance de los fundamentos jurídicos en virtud del artículo 7 y, en especial, el alcance del artículo 7, letra f), son objeto de debate en este momento.

El artículo 6 de la propuesta de Reglamento enumera los supuestos para un tratamiento lícito de los datos personales. Con algunas excepciones (que se especificarán a continuación), los seis fundamentos disponibles permanecen en gran medida sin variación en relación con los estipulados actualmente en el artículo 7 de la Directiva. La Comisión, sin embargo, ha propuesto facilitar directrices adicionales en forma de actos delegados.

Cabe destacar, en el contexto de los trabajos de la correspondiente Comisión del Parlamento Europeo[18], que se ha intentado aclarar el concepto de interés legítimo en la propia propuesta de Reglamento. Se ha elaborado una lista de casos en los que el interés legítimo del responsable del tratamiento de los datos, como norma, prevalecería sobre el interés legítimo y los derechos y libertades fundamentales del interesado, y una segunda lista de casos en los que sucedería lo contrario. Estas listas, recogidas bien en disposiciones bien en considerandos, aportan información de interés en la evaluación del equilibrio entre los derechos e intereses del responsable del tratamiento y del interesado, y se tienen en consideración en el presente Dictamen[19].

16 Véase el artículo 6, apartado 1, del TUE.

17 Véase el artículo 8, apartado 2, de la Carta.

18 Proyecto de informe a la Comisión de Libertades Civiles, Justicia y Asuntos de Interior (LIBE, en sus siglas en inglés) sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo 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 (Reglamento general de protección de datos) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), de 16.1.2013 («Proyecto de informe de la Comisión LIBE»). Véanse, en especial, las enmiendas 101 y 102. Véanse también las enmiendas adoptadas por la Comisión el 21.10.2013 en su informe final («Informe final de la Comisión LIBE»).

19 Véase la sección III.3.1, en particular, los guiones de las páginas 24 y 25, que contienen una lista no exhaustiva de los contextos más comunes en los que puede surgir la cuestión del interés legítimo en virtud del artículo 7, letra f).

II.2. La función del concepto

El interés legítimo del responsable del tratamiento: ¿prueba de sopesamiento como opción final?

El artículo 7, letra f), figura como la última opción de los seis fundamentos que permiten el tratamiento lícito de los datos personales. En dicho apartado se insta a aplicar una *prueba de sopesamiento*: lo que es necesario para el interés legítimo del responsable del tratamiento (o terceros) debe sopesarse en relación con los intereses o los derechos y libertades fundamentales del interesado. El resultado de esta prueba de sopesamiento determinará si el artículo 7, letra f), puede considerarse un fundamento jurídico del tratamiento.

El carácter abierto de esta disposición plantea muchas cuestiones importantes relativas a su aplicación y alcance exactos, que se analizarán a su vez en el presente Dictamen. Sin embargo, tal como se explicará a continuación, esto no significa necesariamente que esta opción deba considerarse como aquella que puede utilizarse con moderación únicamente para cubrir las lagunas en situaciones raras o imprevistas como «un último recurso», o como una última posibilidad si no se pueden utilizar otros fundamentos. Tampoco deberá percibirse como una opción preferente ni deberá extenderse su uso de manera indebida porque se considere menos restrictiva que los demás fundamentos.

Por el contrario, puede afirmarse que el artículo 7, letra f), tiene su propio ámbito natural de pertinencia y desempeña una función muy útil como fundamento jurídico del tratamiento, siempre que se cumplan una serie de condiciones necesarias.

Una utilización apropiada del artículo 7, letra f), en las circunstancias correctas y sujeta a las garantías adecuadas, puede ayudar también a impedir el uso indebido de otros fundamentos jurídicos y a evitar una dependencia excesiva de estos.

Los primeros cinco fundamentos del artículo 7 se basan en el consentimiento del interesado, el acuerdo contractual, la obligación jurídica u otra justificación especialmente identificada como motivo de legitimidad. Cuando el tratamiento se basa en uno de estos cinco fundamentos jurídicos, se considera legítimo *a priori* y, por tanto, solo está sujeto al cumplimiento de las demás disposiciones aplicables de la legislación. En otras palabras, existe una presunción de que se alcanza el equilibrio entre los diferentes derechos e intereses en juego —incluidos los del responsable del tratamiento y los del interesado— asumiendo, por supuesto, que se cumplen las demás disposiciones de la legislación sobre la protección de datos. El artículo 7, letra f), por otro lado, exige un examen *específico*, para casos que no encajan en los escenarios definidos previamente en virtud de los fundamentos de a) a e). De este modo se garantiza que, fuera de estos escenarios, cualquier tratamiento tiene que cumplir el requisito de la prueba de sopesamiento, teniendo en debida consideración los intereses y los derechos fundamentales del interesado.

Este examen puede llevar a la conclusión, en determinados casos, de que la balanza se inclina a favor de los intereses y los derechos fundamentales de los interesados y que, en consecuencia, el tratamiento no puede llevarse a cabo. Por otro lado, una evaluación adecuada del equilibrio en virtud del artículo 7, letra f), en ocasiones con una posibilidad de exclusión voluntaria del tratamiento, puede en otros casos ser una alternativa válida al uso inapropiado, por ejemplo, del fundamento basado en el «consentimiento» o en la «necesidad de ejecución de un contrato». Considerado de este modo, el artículo 7, letra f), presenta garantías

complementarias —que requieren medidas adecuadas— comparado con otros fundamentos determinados previamente. No deberá, por tanto, considerarse como «el vínculo más débil» o una puerta abierta para legitimar todas las actividades de tratamiento de datos que no estén comprendidas en cualquiera de los demás fundamentos jurídicos.

El Grupo de trabajo reitera que al interpretar el alcance del artículo 7, letra f), se aspira a un enfoque equilibrado que garantice la flexibilidad necesaria a los responsables del tratamiento de datos en situaciones en las que no exista un impacto indebido sobre los interesados, mientras que, al mismo tiempo, estos disfruten de una seguridad jurídica y unas garantías suficientes para que esta disposición abierta no se utilice de manera indebida.

II.3. Conceptos relacionados

Relación del artículo 7, letra f), con otros motivos de licitud

El artículo 7 comienza con el consentimiento, y después enumera los demás motivos de licitud, incluidos los contratos y las obligaciones jurídicas, avanzando gradualmente hasta el examen del interés legítimo, que se enumera como el último de los seis fundamentos jurídicos posibles. El orden en el que se enumeran los fundamentos jurídicos de conformidad con el artículo 7 ha sido interpretado a veces como una indicación de la importancia respectiva de los diferentes fundamentos. Sin embargo, tal como se destaca en el Dictamen del Grupo de trabajo sobre el concepto de consentimiento[20], el texto de la Directiva no realiza distinción jurídica alguna entre los seis fundamentos jurídicos y no sugiere que haya una jerarquía entre ellos. No existe ninguna indicación de que el artículo 7, letra f), solo deba aplicarse en casos excepcionales y el texto no sugiere de ningún otro modo que el orden específico de los seis fundamentos jurídicos tenga ningún efecto jurídicamente pertinente. Por otro lado, el significado preciso del artículo 7, letra f), y su relación con otros motivos de licitud ha carecido de claridad durante mucho tiempo.

En estas circunstancias, y teniendo en consideración las diversidades históricas y culturales y el lenguaje abierto de la Directiva, se han adoptado diferentes enfoques: algunos Estados miembros han tendido a percibir el artículo 7, letra f), como el fundamento menos preferido, destinado a cubrir las lagunas solo en algunos casos excepcionales cuando ninguno de los otros cinco fundamentos se aplique o pueda aplicarse[21]. Otros Estados miembros, por el contrario, lo consideran solo una de las seis opciones, ni más ni menos importante que el resto, que puede aplicarse en un gran número y variedad de situaciones, siempre que se cumplan las condiciones necesarias.

Teniendo en consideración estas divergencias, y también a la luz de la sentencia de ASNEF y FECEMD, es importante aclarar la relación del motivo de «interés legítimo» con los demás motivos de licitud —por ejemplo, en relación con el consentimiento, los contratos, las misiones de interés público— y también en relación con el derecho de oposición del interesado. Esto puede ayudar a definir mejor el papel y la función del motivo del interés legítimo y, por tanto, puede contribuir a la seguridad jurídica.

---

20 Véase el pie de página 2 anterior.

21 También debe destacarse que el Proyecto de informe de la Comisión LIBE, en su enmienda 100, propuso separar el artículo 7, letra f), del resto de los fundamentos jurídicos y también propuso requisitos adicionales para el caso de que se utilice este fundamento jurídico, incluidas más transparencia y una mayor responsabilidad, tal como se explicará más adelante.

También debe destacarse que el motivo del interés legítimo, junto con otros fundamentos además del consentimiento, exige un examen de la «necesidad». Esto limita estrictamente el contexto en el que pueden aplicarse cada uno de ellos. El Tribunal de Justicia de la Unión Europea considera que la «necesidad» es un concepto que tiene su propio significado independiente en la legislación comunitaria[22]. El Tribunal Europeo de Derechos Humanos también ha facilitado directrices útiles[23].

Además, utilizar un fundamento jurídico adecuado no exime al responsable del tratamiento de datos de sus obligaciones en virtud del artículo 6 relativas a la imparcialidad, la licitud, la necesidad y la proporcionalidad, así como a la calidad de los datos. Por ejemplo, incluso un tratamiento de datos personales basado en el motivo del interés legítimo o en la ejecución de un contrato no permitiría la recopilación excesiva de datos para un fin específico.

El interés legítimo y los demás fundamentos del artículo 7 son fundamentos alternativos y, por tanto, es suficiente con aplicar uno de ellos. Sin embargo, son acumulativos no solo con los requisitos del artículo 6 sino también con todos los demás principios y requisitos de la protección de datos que puedan ser de aplicación.

Otras pruebas de sopesamiento

El artículo 7, letra f), no es la única prueba de sopesamiento previsto en la Directiva. Por ejemplo, el artículo 9 insta a sopesar el derecho a la protección de los datos personales y la libertad de expresión. Este artículo permite a los Estados miembros establecer las exenciones y excepciones necesarias en lo referente al tratamiento de datos personales «con fines exclusivamente periodísticos o de expresión artística o literaria», «solo en la medida en que resulten necesarias para conciliar el derecho a la intimidad con las normas que rigen la libertad de expresión».

Además, muchas otras disposiciones de la Directiva también exigen un análisis caso por caso, sopesando los intereses y derechos en juego, y realizando una evaluación flexible de diversos factores. Por ejemplo, las disposiciones sobre la necesidad, la proporcionalidad y la limitación de la finalidad, las excepciones del artículo 13 y la investigación científica, por nombrar solo algunas.

En efecto, parece que la Directiva se concibió para dejar margen a la interpretación y al equilibrio de intereses. Esto se hizo al menos en parte, por supuesto, para permitir mayor margen a los Estados miembros al incorporarla al Derecho nacional. Además, no obstante, la

---

22 Sentencia del Tribunal de Justicia de la Unión Europea de 16 de diciembre de 2008 en el asunto C-524/06 (Heinz Huber / Bundesrepublik Deutschland), apartado 52: «Por consiguiente, habida cuenta del objetivo consistente en equiparar el nivel de protección en todos los Estados miembros, el concepto de necesidad, tal como resulta del artículo 7, letra e), de la Directiva 95/46 –cuyo objeto es delimitar con precisión uno de los supuestos en los que resulta lícito el tratamiento de datos personales–, no puede tener un contenido variable en función de los Estados miembros. Por lo tanto, se trata de un concepto autónomo del Derecho comunitario que debe recibir una interpretación idónea para responder plenamente al objeto de dicha Directiva, tal como se define en el artículo 1, apartado 1, de la misma.»

23 Sentencia del Tribunal Europeo de Derechos Humanos en el asunto Silver y otros / el Reino Unido, de 25 de marzo de 1983, apartado 97, debatiendo el concepto «necesario en una sociedad democrática»: «el adjetivo "necesario" no es sinónimo de "indispensable", ni tiene la flexibilidad de las expresiones "admisible", "ordinario", "útil", "razonable" o "deseable"... »

necesidad de cierta flexibilidad también se deriva de la naturaleza misma del derecho a la protección de los datos personales y del derecho a la privacidad. De hecho, estos dos derechos, junto con la mayoría (aunque no todos) de los demás derechos fundamentales, se consideran derechos humanos relativos o cualificados[24]. Estos tipos de derechos deben siempre interpretarse según el contexto. Sujetos a las garantías adecuadas, pueden sopesarse en relación con los derechos de otros. En algunas situaciones, y también sujetos a las garantías adecuadas, pueden restringirse por motivos de interés público.

II.4. Contexto y consecuencias estratégicas

Garantizar tanto la legitimidad como la flexibilidad: instrumentos de especificación del artículo 7, letra f)

El texto actual del artículo 7, letra f), de la Directiva es un texto abierto. Esto significa que se puede utilizar en una amplia variedad de situaciones, siempre que se cumplan sus requisitos, incluida la prueba de sopesamiento. No obstante, esta flexibilidad puede también tener implicaciones negativas. Con el fin de impedir que dicha flexibilidad dé lugar a una aplicación nacional incoherente o a una carencia de seguridad jurídica, resulta fundamental contar con orientaciones adicionales.

La Comisión prevé dichas directrices en la propuesta de Reglamento en forma de actos delegados. Otras opciones incluyen facilitar aclaraciones y disposiciones detalladas en el texto de la propuesta misma de Reglamento[25], o encargar al Consejo Europeo de Protección de Datos la tarea de proporcionar orientaciones adicionales en este ámbito.

Cada una de estas opciones, a su vez, tiene sus beneficios e inconvenientes. Si la evaluación se hiciera caso por caso sin ninguna orientación adicional, se correría el riesgo de una aplicación incoherente y de una falta de previsibilidad jurídica, como ha sido el caso en el pasado.

Por otro lado, si se facilitan, en el texto de la propuesta misma de Reglamento, unas listas detalladas y exhaustivas de situaciones en las que el interés legítimo del responsable del tratamiento prevalezca como norma sobre los derechos fundamentales del interesado y viceversa, se correrá el riesgo de que resulte ambiguo, innecesariamente prescriptivo, o ambas cosas.

Estas aproximaciones podrían inspirar, sin embargo, una solución equilibrada, proporcionando más detalles en la propuesta misma de Reglamento y orientaciones

[24] Existe solo un número reducido de derechos humanos que no pueden sopesarse en relación con los derechos de otros, o con los intereses de la comunidad. Se conocen como derechos absolutos. Estos derechos no pueden nunca limitarse o restringirse, independientemente de las circunstancias, incluso en estado de guerra o de emergencia. Un ejemplo es el derecho a no ser torturado o tratado de manera inhumana o degradante. Nunca es permisible torturar o tratar a alguien de manera inhumana o degradante, independientemente de las circunstancias. Ejemplos de derechos humanos no absolutos comprenden el derecho al respeto de la vida privada y familiar, el derecho a la libertad de expresión y el derecho a la libertad de pensamiento, conciencia y religión.

[25] Véase la sección II.1 Breve historia, bajo el epígrafe «La propuesta de Reglamento de protección de datos», página 10.

adicionales en los actos delegados o en las directrices del Consejo Europeo de Protección de Datos[26].

El análisis del Capítulo III tiene como objetivo sentar las bases con el fin de hallar dicho enfoque, de manera que no sea tan general que carezca de significado, ni tan específico que resulte demasiado rígido.

[26] Respecto a los actos delegados y a las orientaciones del Consejo Europeo de Protección de Datos, el Dictamen 08/2012 del Grupo de trabajo, por el que se facilita más información sobre los debates relativos a la reforma de la protección de datos, adoptado el 5 de octubre de 2001 (WP199), expresaba una preferencia marcada por estas últimas (véanse las páginas 14 y 15).

III. Análisis de las disposiciones

III.1. Sinopsis del artículo 7

El artículo 7 exige que los datos personales sean tratados solamente si es aplicable al menos uno de los seis fundamentos jurídicos enumerados en dicho artículo. Antes de analizar cada uno de estos fundamentos jurídicos, la presente sección III.1 ofrece una sinopsis del artículo 7 y su relación con el artículo 8 sobre categorías especiales de datos.

III.1.1. Consentimiento o «necesario para...»

Puede hacerse una distinción entre el caso de que los datos personales se traten sobre la base del consentimiento inequívoco del interesado (artículo 7, letra a) y los cinco casos restantes artículo 7, letras b) a f). Estos cinco casos, dicho brevemente, describen supuestos en los que el tratamiento puede ser necesario en un contexto específico, como la ejecución de un contrato con el interesado, el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento, etc.

En el primer caso, en virtud del artículo 7, letra a), son los mismos interesados los que autorizan el tratamiento de sus datos personales. La decisión de permitir que sus datos sean tratados depende de ellos. Al mismo tiempo, el consentimiento no elimina la necesidad de respetar los principios estipulados en el artículo 6[27]. Además, el consentimiento todavía tiene que cumplir determinadas condiciones esenciales para ser legítimo, tal como se explica en el Dictamen 15/2011 del Grupo de trabajo[28]. Puesto que tratamiento de los datos del usuario queda en última instancia a su discreción, el énfasis se pone en la validez y el alcance del consentimiento del interesado.

En otras palabras, el primer motivo de legitimación, contenido en el artículo 7, letra a), se centra en la libre determinación del interesado como motivo de legitimación. Los demás fundamentos jurídicos, por el contrario, permiten el tratamiento —sujeto a garantías y medidas— en situaciones en las que, independientemente del consentimiento, resulte apropiado y necesario tratar los datos en un determinado contexto para perseguir un interés legítimo específico.

Las letras b), c), d) y e) especifican cada una un criterio que legitima el tratamiento:

b) la ejecución de un contrato con el interesado;
c) el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento;

---

[27] Sentencia del Tribunal Supremo de los Países Bajos, de 9 de septiembre de 2011, en el asunto ECLI:NL:HR:2011:BQ8097, apartado 3.3, letra e), respecto al principio de proporcionalidad. Véase también la página 8 del Dictamen 15/2011 del Grupo de trabajo, citado en el pie de página 2 anterior: «...la obtención del consentimiento no anula las obligaciones del responsable del tratamiento con arreglo al artículo 6 en lo que respecta a la imparcialidad, necesidad y proporcionalidad, así como a la calidad de los datos. Por ejemplo, incluso un tratamiento de datos personales basado en el consentimiento del usuario no legitimaría la recopilación excesiva de datos para un fin particular».

[28] Véanse también las páginas de 12 a 29 del Dictamen 15/2011 del Grupo de trabajo, citado en el pie de página 2 anterior.

d) la protección del interés vital del interesado;
e) el cumplimiento de una misión de interés público.

La letra f) es menos específica y se refiere, de manera más general, a (cualquier clase de) interés legítimo perseguido por el responsable del tratamiento (en cualquier contexto). Esta disposición general, no obstante, se supedita específicamente a una prueba de sopesamiento adicional cuyo objetivo es proteger los intereses y los derechos de los interesados, tal como se expone a continuación en la sección III.2.

El responsable del tratamiento de datos lleva a cabo inicialmente en todos los casos la evaluación para comprobar si se han cumplido los criterios establecidos en el artículo 7, letras a) a f), sujeta a la legislación aplicable y a las directrices sobre cómo aplicarla. En segunda instancia, la legitimidad del tratamiento puede quedar supeditada a una evaluación adicional, que podrá ser impugnada posiblemente por los interesados, otras partes interesadas, las autoridades de protección de datos y, en último caso dirimirse en los tribunales.

Para completar este breve resumen, debe mencionarse que, tal como se debatirá en la sección III.3.6, al menos en los casos a los que se refieren las letras e) y f), el interesado puede ejercer el derecho de oposición tal como se estipula en el artículo 14[29]. Esto propiciará una nueva evaluación de los intereses en juego o, en el caso de la prospección (artículo 14, letra b)), obligará al responsable del tratamiento a interrumpir el tratamiento de los datos personales sin ninguna evaluación adicional.

III.1.2. Relación con el artículo 8

El artículo 8 de la Directiva regula adicionalmente el tratamiento de determinadas categorías especiales de datos personales. Se aplica específicamente a datos «que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad» (artículo 8, apartado 1, y a datos «relativos a infracciones o condenas penales» (artículo 8, apartado 5).

El tratamiento de dichos datos está en principio prohibido, sujeto a algunas excepciones. El artículo 8, apartado 2, establece una serie de excepciones a dicha prohibición, en las letras de a) a e). El artículo 8, apartados 3 y 4, prevé excepciones complementarias. Algunas de estas disposiciones son similares, aunque no idénticas, a las disposiciones establecidas en el artículo 7, letras a) a f).

Las condiciones específicas del artículo 8, así como el hecho de que algunos de los motivos de legitimación enumerados en el artículo 7 se asemejan a las condiciones establecidas en el artículo 8, plantean la cuestión de la relación entre las dos disposiciones.

Si el artículo 8 está concebido como una *lex specialis*, deberá considerarse si excluye la aplicabilidad del artículo 7 en su conjunto. Si este fuera el caso, esto significaría que las categorías especiales de datos personales pueden tratarse sin cumplir el artículo 7, siempre

[29] De conformidad con el artículo 14, letra a), este derecho se aplica «salvo cuando la legislación nacional disponga otra cosa». Por ejemplo, en la legislación nacional sueca no se permite la posibilidad de oponerse a un tratamiento basado en el artículo 7, letra e).

que sea aplicable una de las excepciones del artículo 8. También es posible, sin embargo, que la relación sea más compleja y que los artículos 7 y 8 deban aplicarse acumulativamente[30].

En cualquier caso, es obvio que el objetivo político es ofrecer protección adicional a las categorías especiales de datos. Por tanto, el resultado final del análisis deberá ser igualmente obvio: la aplicación del artículo 8, tanto en sí misma como de manera acumulativa con el artículo 7, tiene como objetivo proporcionar un nivel mayor de protección a las categorías especiales de datos.

En la práctica, aunque en algunos casos el artículo 8 establece requisitos más estrictos —como el consentimiento «explícito» del artículo 8, apartado 2, letra a), comparado con el «consentimiento inequívoco» del artículo 7—, no sucede lo mismo con todas las disposiciones. Algunas excepciones previstas en el artículo 8 no parecen equivalentes o más estrictas que los fundamentos enumerados en el artículo 7. Resultaría inapropiado concluir, por ejemplo, que el hecho de que se hayan hecho manifiestamente públicas categorías especiales de datos en virtud del artículo 8, apartado 2, letra e), sería —siempre en sí mismo y por sí mismo— una condición suficiente para permitir cualquier tipo de tratamiento de datos sin la evaluación del equilibrio de intereses y derechos en juego exigida en el artículo 7, letra f)[31].

En algunas situaciones, el hecho de que el responsable del tratamiento de datos sea un partido político también levantaría la prohibición del tratamiento de categorías especiales de datos en virtud del artículo 8, apartado 2, letra d). Esto, sin embargo, no significa que cualquier tratamiento dentro del ámbito de dicha disposición sea necesariamente lícito. Deberá evaluarse por separado y el responsable del tratamiento deberá demostrar, por ejemplo, que el tratamiento de los datos es necesario para la ejecución de un contrato (artículo 7, letra b)), o que prevalece su interés legítimo en virtud del artículo 7, letra f). En este último caso, deberá llevarse a cabo la prueba de sopesamiento en virtud del artículo 7, letra f), después de que se haya evaluado si el responsable del tratamiento de los datos cumple los requisitos del artículo 8.

De igual modo, el mero hecho de que «el tratamiento de datos resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios», y que dichos datos sean tratados de conformidad con una obligación de secreto profesional —tal como se establece en el artículo 8, apartado 3— implica que dicho tratamiento de datos sensibles está *exento de la prohibición* del artículo 8, apartado 1. No obstante, esto no es necesariamente suficiente para garantizar también la legalidad en virtud del artículo 7, y exigirá un fundamento jurídico como un contrato con el paciente de conformidad con su letra b), una obligación jurídica con arreglo a su letra c), el

[30] Puesto que el artículo 8 se establece como una prohibición con excepciones, estas excepciones pueden considerarse requisitos que solo limitan el alcance de la prohibición pero que, en sí mismas y por sí mismas, no ofrecen un motivo de legitimación suficiente para el tratamiento. En este sentido, la aplicabilidad de las excepciones del artículo 8 no excluye la aplicabilidad de los requisitos del artículo 7, y ambos, cuando así proceda, deberán aplicarse acumulativamente.

[31] Además, el artículo 8, apartado 2, letra e), no deberá interpretarse a contrario en el sentido de que, cuando los datos hechos públicos por el interesado no sean sensibles, puedan ser tratados sin ninguna condición adicional. Los datos públicamente disponibles siguen siendo datos personales sujetos a los requisitos de la protección de datos, incluido el cumplimiento del artículo 7, independientemente de si se trata o no de datos sensibles.

cumplimiento de una misión de interés público conforme a su letra e) o una evaluación en virtud de su letra f).

En conclusión, el Grupo de trabajo considera que tiene que llevarse a cabo un análisis caso por caso, tanto si el artículo 8 en sí mismo establece condiciones suficientes y más estrictas[32], como si se exige una aplicación acumulativa de ambos artículos 8 y 7 para garantizar la completa protección de los interesados. En ningún caso el resultado de este examen podrá tener como consecuencia una protección menor de estas categorías especiales de datos[33].

Esto también significa que un responsable que esté tratando categorías especiales de datos no podrá nunca invocar *únicamente* un fundamento jurídico en virtud del artículo 7 para legitimar su actividad de tratamiento de datos. Cuando sea aplicable, el artículo 7 no *prevalecerá* sino que se aplicará siempre de manera *acumulativa* con el artículo 8 con el fin de garantizar que se cumplen todas las garantías y medidas pertinentes. Esto será aún más pertinente en el caso de que los Estados miembros decidan añadir exenciones adicionales a aquellas establecidas en el artículo 8, tal como se prevé en su apartado 4.

III.2. Artículo 7, letras a) a e)

Esta sección III.2 ofrece una breve sinopsis de cada uno de los fundamentos especificados en el artículo 7, letras a) a e), de la Directiva, antes de que el Dictamen se centre, en la sección III.3, en el artículo 7, letra f). Este análisis también pondrá de relieve algunas de las interfaces más comunes entre estos fundamentos jurídicos, por ejemplo, entre «contrato», «obligación jurídica» e «interés legítimo», dependiendo del contexto particular y de los hechos del caso.

III.2.1. Consentimiento

El consentimiento como fundamento jurídico ha sido analizado en el Dictamen 15/2011 del Grupo de trabajo sobre la definición del consentimiento. Las principales conclusiones del Dictamen son que el consentimiento es uno de los diversos fundamentos jurídicos para tratar los datos personales, y no el principal motivo. Desempeña un importante papel, pero no excluye la posibilidad, dependiendo del contexto, de que otros fundamentos jurídicos puedan ser más apropiados tanto desde la perspectiva del responsable del tratamiento como desde la perspectiva del interesado. Si se utiliza correctamente, el consentimiento es una herramienta que proporciona al interesado control sobre el tratamiento de sus datos. Si se utiliza incorrectamente, el control del interesado resulta ilusorio y el consentimiento constituye un fundamento inadecuado para el tratamiento.

Entre sus recomendaciones, el Grupo de trabajo insistió en la necesidad de aclarar lo que significa «consentimiento inequívoco»: «La clarificación debería subrayar que el consentimiento inequívoco exige utilizar mecanismos que no dejen lugar a dudas sobre la

[32] Véase el análisis llevado a cabo en el Dictamen sobre la AMA del Grupo de trabajo, punto 3.3, que tiene en consideración tanto el artículo 7 como el artículo 8 de la Directiva: Segundo Dictamen 4/2009 sobre la Norma internacional para la protección de la intimidad y los datos personales de la Agencia Mundial Antidopaje (AMA), sobre disposiciones relacionadas del Código AMA y sobre otros aspectos relacionados con la intimidad en el contexto de la lucha contra el dopaje en el deporte por parte de la AMA y de las organizaciones nacionales antidopaje, adoptado el 6 de abril de 2009 (WP162).

[33] No hace falta decir que también en el caso de aplicación del artículo 8 debe garantizarse el respeto de las demás disposiciones de la Directiva, incluido el artículo 6.

intención de dar su consentimiento del interesado. Al mismo tiempo habría que aclarar que la utilización de opciones por defecto que el interesado debe modificar para negarse al tratamiento (consentimiento basado en el silencio) no constituye consentimiento inequívoco. Así sucede sobre todo en el contexto de Internet »[34]. También exigió que los responsables del tratamiento de los datos establezcan mecanismos para demostrar la obtención del consentimiento (en el marco de una obligación general de responsabilidad) e instó al legislador a añadir un requisito explícito relativo a la calidad y a la accesibilidad de la información que constituye la base del consentimiento.

III.2.2 Contrato

El artículo 7, letra b), establece un fundamento jurídico en situaciones en las que «el tratamiento es necesario para la ejecución de un contrato en el que el interesado sea parte o para la aplicación de medidas precontractuales adoptadas a petición del interesado». Este apartado comprende, así pues, dos escenarios diferentes.

i) En primer lugar, esta disposición abarca situaciones en las que el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte. Esto podría incluir, por ejemplo, el tratamiento de la dirección del interesado, de manera que los bienes adquiridos en línea puedan ser entregados, o el tratamiento de los datos de la tarjeta de crédito con el fin de efectuar un pago. En el contexto del empleo este fundamento jurídico puede permitir, por ejemplo, el tratamiento de la información salarial y de los datos de la cuenta bancaria, de manera que se pueda abonar el salario.

   Esta disposición debe interpretarse de manera estricta y no comprende situaciones en las que el tratamiento no sea realmente *necesario* para la ejecución de un contrato, sino unilateralmente impuesto al interesado por parte del responsable del tratamiento. Además, el hecho de que el tratamiento de algunos datos esté cubierto por un contrato no quiere decir automáticamente que el tratamiento sea necesario para su ejecución. Por ejemplo, el artículo 7, letra b), no es un fundamento jurídico apropiado para elaborar un perfil de los gustos y las opciones de estilo de vida del usuario, basado en su recorrido por un sitio web y en los artículos adquiridos. Ello se debe a que el responsable del tratamiento de los datos no ha sido contratado para elaborar perfiles, sino para entregar bienes y ofrecer servicios concretos, por ejemplo. Incluso si estas actividades de tratamiento se mencionan de manera específica en la letra pequeña del contrato, este hecho por sí solo no las convierte en «necesarias» para la ejecución del contrato.

   Existe una clara relación entre la valoración de la necesidad y el cumplimiento del principio de limitación de la finalidad. Es importante determinar la *justificación* exacta del contrato, es decir, su esencia y objetivo fundamental, ya que la evaluación para comprobar si el tratamiento de datos es necesario para su ejecución se realizará en función de esta información.

   En algunas situaciones dudosas puede ser discutible, o puede requerirse más indagación específica con el fin de determinar si el tratamiento es necesario para la ejecución del contrato. Por ejemplo, la creación de una base interna de datos de

[34] Véase la página 40 del Dictamen 15/2011 del Grupo de trabajo sobre la definición del consentimiento.

contacto de los empleados de una empresa que contenga el nombre, la dirección laboral, el número de teléfono y la dirección de correo electrónico de todos los empleados, para permitir que los empleados puedan ponerse en contacto con sus compañeros de trabajo, puede en determinadas situaciones considerarse como necesario para la ejecución de un contrato en virtud del artículo 7, letra b), pero también podría ser lícito en virtud del artículo 7, letra f), si se demuestra que prevalece el interés del responsable del tratamiento y se toman todas las medidas adecuadas, incluida, por ejemplo, la consulta a los representantes de los empleados.

Otros casos, por ejemplo, la supervisión electrónica del uso del teléfono, del correo electrónico y de Internet por parte de los empleados, o la videovigilancia de los empleados, constituyen más claramente un tipo de tratamiento que es probable que exceda de lo que se estima necesario para la ejecución de un contrato de trabajo, aunque esto puede depender en este caso también de la naturaleza del empleo. La prevención del fraude —que puede comprender, entre otros, la supervisión y la elaboración de perfiles de clientes— es otro ámbito típico que es probable se considere que excede de lo que se estima necesario para la ejecución de un contrato. Dicho tratamiento podría ser en tal caso legítimo en virtud de otro fundamento jurídico del artículo 7, por ejemplo, el consentimiento cuando así proceda, una obligación jurídica o el interés legítimo del responsable del tratamiento (artículo 7, letras a), c) y f))[35]. En este último caso, el tratamiento deberá quedar sujeto a garantías y medidas adicionales para proteger adecuadamente los intereses o los derechos y libertades de los interesados.

El artículo 7, letra b), solo se aplica a lo que es necesario para la *ejecución* de un contrato. No se aplica al resto de acciones desencadenadas por el incumplimiento o por los demás incidentes que se produzcan en la ejecución de un contrato. En la medida en que el tratamiento comprenda la ejecución normal de un contrato, podría entrar en el ámbito del artículo 7, letra b). Si se produjera un incidente en la ejecución que diera lugar a un conflicto, podría adoptarse una medida diferente respecto al tratamiento de los datos. Al tratar la información básica del interesado, como el nombre, la dirección y la referencia a las obligaciones contractuales pendientes, debe considerarse que el envío de recordatorios formales entra todavía en el ámbito del tratamiento de los datos necesarios para la ejecución de un contrato. En relación con un tratamiento de datos más elaborado, que pueda implicar o no a terceros, como el cobro externo de deudas o demandar a un cliente que ha incumplido el pago por un servicio ante los tribunales, podría argumentarse que dicho tratamiento no tiene lugar ya conforme a la ejecución «normal» del contrato y, por tanto, no entraría en el ámbito del artículo 7, letra b). No obstante, esto no haría que el tratamiento fuera ilegítimo como tal: el responsable del tratamiento de datos tiene un interés legítimo en buscar vías de recurso para garantizar que se respetan sus derechos contractuales. Podrían

[35] Otro ejemplo de fundamentos jurídicos múltiples puede encontrarse en el Dictamen 15/2011 del Grupo de trabajo sobre la definición del consentimiento (citado en el pie de página 2). Para la compra de un automóvil, el responsable del tratamiento de datos puede estar autorizado para tratar datos personales con diversos fines y sobre la base de diversos motivos de legitimación:
- datos necesarios para la compra del automóvil: artículo 7, letra b),
- para tramitar los documentos del vehículo: artículo 7, letra c),
- para los servicios de gestión de clientes (por ejemplo, para que el automóvil esté disponible en diferentes empresas filiales dentro de la UE): artículo 7, letra f),
- para transferir los datos a terceros para sus propias actividades de comercialización: artículo 7, letra a).

utilizarse otros fundamentos jurídicos, como el artículo 7, letra f), sujetos a las garantías y medidas adecuadas y al cumplimiento de la prueba de sopesamiento[36].

ii) En segundo lugar, el artículo 7, letra b), también comprende el tratamiento que tiene lugar para la aplicación de medidas *precontractuales*. Esto abarca las relaciones precontractuales, siempre que las medidas se adopten a petición del interesado, y no a iniciativa del responsable del tratamiento o de un tercero. Por ejemplo, si un individuo solicita a un minorista que le envíe una oferta de un producto, el tratamiento con estos fines, como el mantenimiento de los datos de la dirección y de la información sobre la que se ha hecho la solicitud, durante un periodo limitado de tiempo, será adecuado en virtud de este fundamento jurídico. De igual modo, si un individuo solicita un presupuesto de la empresa de seguros de su automóvil, esta puede procesar los datos necesarios, por ejemplo, el modelo y la antigüedad del vehículo, y otros datos pertinentes y proporcionados, con el fin de preparar el presupuesto.

Sin embargo, las verificaciones de antecedentes detalladas, por ejemplo, el tratamiento de datos de reconocimientos médicos antes de que la empresa de seguros ofrezca un seguro de vida o de asistencia sanitaria a un solicitante no se considerarían como medidas necesarias adoptadas a petición del interesado. Las verificaciones de referencias de crédito antes de la concesión de un préstamo tampoco se hacen a *petición* del interesado en virtud del artículo 7, letra b), sino en virtud del artículo 7, letra f), o de su letra c), en cumplimiento de la obligación legal de los bancos de consultar una lista oficial de deudores registrados.

La prospección a iniciativa del minorista o del responsable del tratamiento no será tampoco posible basándose en este fundamento jurídico. En algunos casos, el artículo 7, letra f), podría proporcionar un fundamento jurídico adecuado en vez de la letra b), sujeto a las garantías y medidas adecuadas y a la prueba de sopesamiento. En otros casos, incluidos aquellos que implican una elaboración de perfiles generalizada, información compartida, prospección en línea o publicidad basada en el comportamiento, se deberá considerar el consentimiento en virtud del artículo 7, letra a), tal como se desprende del análisis que se expone a continuación[37].

[36] Con respecto a las categorías especiales de datos, también debe tenerse en cuenta el artículo 8, apartado 2, letra e) («necesario para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial»).

[37] Véase la sección III.3.6, letra b), bajo el epígrafe «Ejemplo: la evolución en el enfoque de la prospección », en las páginas 53 y 54.

III.2.3. Obligación jurídica

El artículo 7, letra c), establece un fundamento jurídico en situaciones en las que el «tratamiento es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento». Este puede ser el caso, por ejemplo, cuando los empleadores deban informar de los datos salariales de sus empleados a la seguridad social o a las autoridades fiscales, o cuando las instituciones financieras estén obligadas a informar sobre determinadas transacciones sospechosas a las autoridades competentes en virtud de la normativa contra el blanqueo de dinero. También podría tratarse de una obligación a la que esté sujeta la autoridad pública, ya que nada limita la aplicación del artículo 7, letra c), al sector privado o público. Esto podría aplicarse, por ejemplo, a la recopilación de datos por parte de una autoridad local para la gestión de las multas de aparcamiento en lugares no autorizados.

El artículo 7, letra c), presenta similitudes con su letra e), ya que una misión de interés público se basa con frecuencia o se desprende de una disposición jurídica. El ámbito del artículo 7, letra c), se encuentra, no obstante, estrictamente delimitado.

Para que se aplique el artículo 7, letra c), la obligación debe estar prevista en la ley (y no en un acuerdo contractual, por ejemplo). Dicha ley debe cumplir todas las condiciones pertinentes para que la obligación sea válida y vinculante, y debe también acatar la legislación de protección de datos, incluido el requisito de necesidad, proporcionalidad[38] y limitación de la finalidad.

También es importante destacar que el artículo 7, letra c), se refiere a la legislación de la Unión Europea o de un Estado miembro. Las obligaciones de conformidad con las leyes de terceros países (tales como, por ejemplo, la obligación de establecer regímenes internos de denuncia de irregularidades en virtud de la ley Sarbanes–Oxley de 2002 en Estados Unidos) no están cubiertas por este fundamento jurídico. Para que sea válida, una obligación jurídica de un tercer país necesitaría estar oficialmente reconocida e integrada en el orden jurídico del Estado miembro en cuestión, por ejemplo, en forma de un acuerdo internacional[39]. Por otro lado, la necesidad de cumplir una obligación extranjera puede representar un interés legítimo del responsable del tratamiento, pero solo sujeta a la prueba de sopesamiento del artículo 7, letra f), y siempre que se prevean las garantías adecuadas, tales como las aprobadas por la autoridad competente de protección de datos.

El responsable del tratamiento no debe poder elegir si cumple o no dicha obligación. Las asociaciones público-privadas y los compromisos unilaterales voluntarios con arreglo a los cuales se pueda realizar un tratamiento de datos que exceda lo que exige la ley no están cubiertos, por tanto, por el artículo 7, letra c). Por ejemplo, en el caso de que —sin una clara y

---

38 Véase también el Dictamen 01/2014 del Grupo de trabajo sobre la aplicación de los conceptos de necesidad y proporcionalidad y la protección de datos en el sector de los organismos con funciones coercitivas, adoptado el 27 de febrero de 2014 (WP 211).

39 Véase sobre esta cuestión la sección 4.2.2 del Dictamen 10/2006 del Grupo de trabajo sobre el tratamiento de datos personales por parte de la Sociedad de Telecomunicaciones Financieras Interbancarias Mundiales (Worldwide InterbankFinancial Telecommunication - SWIFT) adoptado el 22 de noviembre de 2006 (WP128), y el Dictamen 1/2006 del Grupo de trabajo relativo a la aplicación de las normas sobre protección de datos de la UE a los sistemas internos de denuncia de irregularidades en los ámbitos de la contabilidad, controles de auditoría internos, cuestiones de auditoría, lucha contra la corrupción y delitos financieros y bancarios, adoptado el 1 de febrero de 2006 (WP 117).

específica obligación jurídica al respecto— un proveedor de servicios de Internet decidiera supervisar a sus usuarios en un esfuerzo por combatir las descargas ilegales, el artículo 7, letra c), no constituirá un fundamento jurídico apropiado para este fin.

Además, la propia obligación legal debe estar suficientemente clara en lo que respecta al tratamiento de los datos personales que se requiere. Por tanto, el artículo 7, letra c), es aplicable sobre la base de las disposiciones jurídicas que hacen referencia explícitamente a la naturaleza y al objeto del tratamiento. El responsable del tratamiento no deberá tener un grado indebido de discreción sobre cómo cumplir con dicha obligación jurídica.

La legislación puede, en algunos casos, establecer solo un objetivo general, al tiempo que se imponen obligaciones más específicas en un nivel diferente, por ejemplo, bien en el Derecho derivado legislación secundaria bien en una decisión vinculante de una autoridad pública en un caso concreto. Esto puede también implicar obligaciones jurídicas en virtud del artículo 7, letra c), siempre que la naturaleza y el objeto del tratamiento estén bien definidos y sujetos a una base jurídica adecuada.

No obstante, esto es diferente si una autoridad reguladora solo proporciona directrices y condiciones políticas generales en virtud de las cuales podría considerar el uso de sus facultades coercitivas (por ejemplo, directrices normativas para las instituciones financieras sobre determinadas normas de diligencia debida). En estos casos, las actividades de tratamiento deberán evaluarse en virtud del artículo 7, letra f), y considerarse legítimas únicamente si quedan supeditadas a una prueba de sopesamiento adicional[40].

Como observación general, cabe mencionar que puede parecer que algunas actividades de tratamiento están próximas al ámbito del artículo 7, letras c) o b), sin que se cumplan los criterios para que se apliquen estos fundamentos jurídicos. Esto no significa que dicho tratamiento sea siempre necesariamente ilícito: puede a veces ser legítimo, pero en virtud de la letra f) del artículo, es decir, supeditado a una prueba de sopesamiento adicional.

III.2.4. Interés vital

El artículo 7, letra d), establece un fundamento jurídico en situaciones en las que «el tratamiento es necesario para proteger el interés vital del interesado». Esta redacción es diferente del lenguaje utilizado en el artículo 8, apartado 2, letra c), más específico y que se refiere a situaciones en las que «el tratamiento sea necesario para salvaguardar el interés vital del interesado o de otra persona, en el supuesto de que el interesado esté física o jurídicamente incapacitado para dar su consentimiento».

Ambas disposiciones, no obstante, parecen sugerir que este fundamento jurídico debería tener una aplicación limitada. En primer lugar, el concepto de «interés vital» parece limitar la aplicación de este fundamento jurídico a cuestiones de vida o muerte, o como mínimo, a amenazas que supongan un riesgo de lesiones u otro daño para la salud del interesado (o en el caso del artículo 8, apartado 2, letra c), también de otra persona).

[40] Las directrices por parte de la autoridad reguladora pueden seguir desempeñando una función a la hora de evaluar el interés legítimo del responsable del tratamiento (véase la sección III.3.4, letra a), en especial la página 42).

El considerando 31 confirma que el objetivo de este fundamento jurídico es «proteger un interés esencial para la vida del interesado». No obstante, la Directiva no especifica de manera precisa si la amenaza debe ser inmediata. Esto plantea cuestiones relativas al ámbito de la recopilación de los datos, por ejemplo, si se trata de una medida preventiva o a gran escala, tales como la recopilación de los datos de los pasajeros de una línea aérea cuando existe un riesgo de enfermedad epidemiológica o se ha detectado un incidente de seguridad.

El Grupo de trabajo considera que debe hacerse una interpretación restrictiva de esta disposición, respetando el espíritu del artículo 8. Aunque el artículo 7, letra d), no limita específicamente el uso de este fundamento jurídico a situaciones en las que el consentimiento no puede utilizarse como fundamento jurídico por los motivos especificados en el artículo 8, apartado 2, letra c), es razonable suponer que en situaciones en las que exista la posibilidad y la necesidad de solicitar un consentimiento válido, el consentimiento deberá, por supuesto, solicitarse siempre que sea posible. Esto también limitaría la aplicación de esta disposición a un análisis caso por caso y no puede normalmente utilizarse para legitimar cualquier recopilación o tratamiento masivos de datos personales. En caso de que esto resultara necesario, las letras c) o e) del artículo 7 serían motivos de legitimación más apropiados para el tratamiento.

III.2.5. Misión de interés público

El artículo 7, letra e), proporciona un fundamento jurídico en situaciones en las que «el tratamiento es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos».

Es importante destacar que, así como la letra c), también el artículo 7, letra e), se refiere al interés público de la Unión Europea o de un Estado miembro. De igual modo, «poder público» se refiere a una autoridad conferida por la Unión Europea o un Estado miembro. En otras palabras, las misiones llevadas a cabo en el interés público de un tercer país o en el ejercicio de una autoridad oficial conferida en virtud de la legislación extranjera no entran dentro del ámbito de esta disposición[41].

El artículo 7, letra e), cubre dos situaciones y es pertinente tanto para el sector público como para el sector privado. En primer lugar, comprende situaciones en las que el mismo responsable del tratamiento tiene una potestad pública o una misión de interés público (pero no necesariamente una obligación jurídica de tratar los datos) y el tratamiento es necesario para el ejercicio de dicha potestad o para la ejecución de dicha misión. Por ejemplo, una autoridad fiscal puede recopilar y tratar la declaración de la renta de una persona física con el fin de establecer y verificar el importe del impuesto pagadero. O una asociación profesional como un colegio de abogados o un colegio de profesionales médicos al que se ha conferido un poder oficial para hacerlo puede llevar a cabo procedimientos disciplinarios contra algunos de sus miembros. Otro ejemplo podría ser un organismo gubernamental local, como una autoridad municipal, a la que se encarga la tarea de gestionar un servicio de biblioteca, un colegio o una piscina local.

---

41 Véase la sección 2.4 del documento de trabajo del Grupo de trabajo relativo a una interpretación común del artículo 26, apartado 1, de la Directiva 95/46/CE, de 24 de octubre de 1995, adoptado el 25 de noviembre de 2005, (WP114) para una interpretación similar del concepto de «interés público importante» en el artículo 26, apartado 1, letra d).

En segundo lugar, el artículo 7, letra e), también comprende situaciones en las que el responsable del tratamiento no tiene una potestad oficial, pero una tercera parte con dicha potestad le solicita que revele los datos. Por ejemplo, un funcionario de un organismo público competente para investigar delitos puede pedir al responsable del tratamiento que coopere en una investigación en curso, en vez de ordenar al responsable del tratamiento que cumpla una solicitud específica de cooperación. El artículo 7, letra e), cubre además situaciones en las que el responsable del tratamiento comunica de forma proactiva los datos a una tercera parte con dicha potestad oficial. Este puede ser el caso, por ejemplo, de que el responsable del tratamiento advierta que se ha cometido un delito penal y facilite esta información a las autoridades competentes con funciones coercitivas por iniciativa propia.

A diferencia del caso del artículo 7, letra c), no se exige que el responsable del tratamiento actúe en virtud de una obligación jurídica. Utilizando el ejemplo anterior, puede que un responsable del tratamiento que advierta de manera accidental que se ha cometido un robo o un fraude no tenga la obligación jurídica de informar de ello a la policía pero puede, no obstante, en determinados casos, hacerlo así voluntariamente de conformidad con el artículo 7, letra e).

No obstante, el tratamiento debe ser «necesario para el cumplimiento de una misión de interés público». Alternativamente, se debe haber conferido un poder oficial bien al responsable del tratamiento bien a la tercera parte a la que este comunica los datos y el tratamiento de datos debe ser necesario para el ejercicio de dicha potestad[42]. También resulta importante poner de relieve que este poder oficial o misión de interés público deberán conferirse o atribuirse normalmente mediante leyes ordinarias u otra normativa jurídica. Si el tratamiento conlleva una invasión de la privacidad o si este se exige de otro modo en virtud de la legislación nacional para garantizar la protección de las personas afectadas, la base jurídica deberá ser lo suficientemente específica y precisa a la hora de definir el tipo de tratamiento de datos que puede permitirse.

Estas situaciones son cada vez más comunes, también fuera de los límites del sector público, si tenemos en consideración la tendencia a la subcontratación de tareas gubernamentales a entidades del sector privado. Este puede ser el caso, por ejemplo, en el contexto del tratamiento de datos en los sectores del transporte o la sanidad (por ejemplo, estudios epidemiológicos, investigación). Este fundamento jurídico también podría invocarse en un contexto policial, tal como ya se ha sugerido en los ejemplos anteriores. Sin embargo, la medida en la que se puede permitir que una empresa privada coopere con las autoridades con funciones coercitivas, por ejemplo, en la lucha contra el fraude o los contenidos ilegales en Internet, exige un análisis no solo en virtud del artículo 7 sino también conforme al artículo 6, teniendo en consideración los requisitos de limitación de la finalidad, imparcialidad y legalidad[43].

---

[42] En otras palabras, en estos casos la importancia pública de las tareas y la responsabilidad correspondiente continuará estando presente incluso si la realización de ese cometido se ha transferido a otras entidades, incluidas entidades privadas.

[43] Véase, en este sentido, el Dictamen del Grupo de trabajo sobre SWIFT (citado en el pie de página 39 anterior), el Dictamen del Grupo de trabajo 4/2003 relativo al nivel de protección garantizado en los EE.UU. para la transferencia de datos de pasajeros, aprobado el 13 de junio de 2003 (WP78) y el Documento de trabajo sobre cuestiones relativas a la protección de datos relacionadas con los derechos de propiedad intelectual, aprobado el 18 de enero de 2005 (WP 104).

El artículo 7, letra e), tiene, en teoría, un ámbito muy amplio de aplicación, que requiere una interpretación estricta y una clara identificación, caso por caso, del interés público en juego y de la potestad oficial que justifica el tratamiento. Este amplio ámbito de aplicación también explica el motivo por el que, al igual que para el artículo 7, letra f), se ha previsto un derecho de oposición en el artículo 14 cuando el tratamiento se basa en el artículo 7, letra e)[44]. Pueden aplicarse, por tanto, garantías y medidas adicionales similares en ambos casos [45].

En este sentido, el artículo 7, letra e), tiene similitudes con la letra f) del mismo, y en algunos contextos, especialmente los referidos a las autoridades públicas, la letra e) puede reemplazar al artículo 7, letra f).

Cuando se evalúe el alcance de estas disposiciones para los organismos del sector público, especialmente a la luz de los cambios propuestos en el marco jurídico de la protección de datos, es útil destacar que el texto actual del Reglamento nº 45/2001[46], que contiene las normas de protección de datos aplicables a las instituciones y los organismos de la Unión Europea, no tiene ninguna disposición comparable al artículo 7, letra f).

Sin embargo, el considerando 27 de este Reglamento estipula que «el tratamiento de datos personales efectuado a cargo de las instituciones y organismos comunitarios para la realización de las tareas *de interés público* incluye el tratamiento de datos personales necesarios para la gestión y el funcionamiento de dichas instituciones y organismos». Esta disposición permite, por tanto, el tratamiento de datos basado en un fundamento jurídico interpretado de manera amplia como «tarea de interés público» en una gran variedad de casos, que podrían de otro modo haber sido cubiertos por una disposición similar al artículo 7, letra f). La videovigilancia de las instalaciones con fines de seguridad, la supervisión electrónica del tráfico de correo electrónico o las evaluaciones del personal son solo algunos ejemplos de lo que puede entrar dentro del ámbito de esta disposición interpretada de manera amplia como «misiones de interés público».

De cara al futuro, también es importante considerar que la propuesta de Reglamento, en su artículo 6, apartado 1, letra f), estipula de manera específica que el motivo del interés legítimo «no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones». Si esta disposición se promulga y se interpreta de manera amplia, de forma que las autoridades públicas en su conjunto estén excluidas de la aplicación del interés legítimo como fundamento jurídico , entonces los motivos de «interés público» y «poder oficial» del artículo 7, letra e), deberán interpretarse de manera que permitan a las autoridades públicas cierto grado de flexibilidad, al menos con el fin de garantizar su gestión y funcionamiento adecuados, exactamente del mismo modo en que se interpreta el Reglamento nº 45/2001 en la actualidad.

---

44 Tal como se menciona anteriormente, esta posibilidad de oposición no existe en algunos Estados miembros (por ejemplo, Suecia) para el tratamiento de datos basado en el artículo 7, apartado e).

45 Como se expondrá a continuación, el Proyecto de informe de la Comisión LIBE sugirió garantías adicionales —en especial, el aumento de la transparencia— para los casos en los que aplique el artículo 7, letra f).

46 Reglamento (CE) n° 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos (DO L 8, 12.1.2001, p. 1).

Alternativamente, la última frase del artículo 6, apartado 1, letra f), de la propuesta de Reglamento a la que se hace referencia podría interpretarse de manera que no excluya a las autoridades públicas en su conjunto de la utilización del interés legítimo como fundamento jurídico. En este caso, la frase «tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones» en el artículo 6, apartado 1, letra f) propuesto, deberá interpretarse en sentido estricto. Esta interpretación estricta significaría que el tratamiento para la gestión y el funcionamiento adecuados de estas autoridades públicas se encontraría fuera del ámbito del «tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones». Como consecuencia, el tratamiento para la gestión y el funcionamiento adecuados de estas autoridades públicas podría todavía ser posible en virtud del motivo del interés legítimo.

III.3. Artículo 7, letra f): interés legítimo

El artículo 7, letra f)[47], insta a aplicar una prueba de sopesamiento: el interés legítimo del responsable del tratamiento (o terceros) debe sopesarse en relación con los intereses o los derechos y libertades fundamentales del interesado. El resultado de esta prueba determinará en gran medida si el artículo 7, letra f), puede considerarse un fundamento jurídico del tratamiento.

Cabe señalar ya en este estadio que no se trata de una prueba de sopesamiento directa que consista simplemente en ponderar dos «pesos» fácilmente cuantificables y comparables. Por el contrario, como se explicará con más detalle posteriormente, llevar a cabo esta prueba de sopesamiento puede exigir una compleja evaluación que tenga en consideración una serie de factores. Con el fin de ayudar a estructurar y simplificar dicha evaluación, hemos desglosado el proceso en varios pasos para facilitar que la prueba de sopesamiento se efectúe de manera eficaz.

En la sección III.3.1 se examina, en primer lugar, un lado de la balanza: lo que constituye «el interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos». En la sección III.3.2, se examina el otro lado de la balanza: lo que constituyen «los intereses o los derechos y libertades fundamentales del interesado que requieran protección en virtud del apartado 1 del artículo 1».

En las secciones III.3.3 y III.3.4 se proporcionan directrices sobre la manera de efectuar la prueba de sopesamiento. En la sección III.3.3 se ofrece una introducción general con la ayuda de tres escenarios diferentes. Después de esta introducción, en la sección III.3.4 se describen las consideraciones más importantes que deben tenerse en cuenta a la hora de efectuar la prueba de sopesamiento, incluidas las garantías y las medidas adoptadas por el responsable del tratamiento de datos.

En las secciones III.3.5 y III.3.6, por último, también se examinan determinados mecanismos especiales, tales como la responsabilidad, la transparencia y el derecho de oposición, que pueden garantizar por —y reforzar — un adecuado equilibrio de los diversos intereses que estén en juego.

III.3.1. Interés legítimo del responsable del tratamiento (o terceros)

[47] El texto completo del artículo 7, letra f), puede consultarse en la página 5 anterior.

El concepto de «interés»

El concepto de «interés» está estrechamente relacionado con el concepto de «finalidad» mencionado en el artículo 6 de la Directiva, aunque se trata de conceptos diferentes. En términos de protección de datos, «finalidad» es la razón específica por la que se tratan los datos: el objetivo o la intención del tratamiento de los datos. Un interés, por otro lado, se refiere a una mayor implicación que el responsable del tratamiento pueda tener en el tratamiento, o al beneficio que el responsable del tratamiento obtenga —o que la sociedad pueda obtener— del tratamiento.

Por ejemplo, una empresa puede tener un *interés* en garantizar la salud y seguridad del personal que trabaje en su central nuclear. Por consiguiente, la empresa puede tener como *finalidad* la aplicación de procedimientos de control de acceso específicos que justifique el tratamiento de determinados datos personales específicos con el fin de velar por la salud y la seguridad del personal.

Un interés debe estar articulado con la claridad suficiente para permitir que la prueba de sopesamiento se lleve a cabo en contraposición a los intereses y los derechos fundamentales del interesado. Además, el interés en juego debe también ser «perseguido por el responsable del tratamiento». Esto exige un interés real y actual, que se corresponda con actividades presentes o beneficios que se esperen en un futuro muy próximo. En otras palabras, los intereses que sean demasiado vagos o especulativos no serán suficientes.

La naturaleza del interés puede variar. Algunos intereses pueden ser apremiantes y beneficiosos para la sociedad en general, tales como el interés de la prensa en publicar información sobre la corrupción gubernamental o el interés en llevar a cabo investigación científica (sujetos a las garantías adecuadas). Otros intereses pueden ser menos apremiantes para la sociedad en su conjunto o, en cualquier caso, el impacto de su búsqueda en la sociedad puede ser más dispar o controvertido. Esto puede, por ejemplo, aplicarse al interés económico de una empresa en aprender tanto como sea posible sobre sus potenciales clientes con el fin de orientar mejor la publicidad sobre sus productos y servicios.

¿Qué convierte a un interés en «legítimo» o «ilegítimo»?

El objetivo de esta pregunta es identificar el umbral de lo que constituye un interés legítimo. Si el interés del responsable del tratamiento de datos es ilegítimo no deberá aplicarse la prueba de sopesamiento, puesto que no se habrá alcanzado el umbral inicial para la utilización del artículo 7, letra f).

En opinión del Grupo de trabajo, el concepto de interés legítimo podría comprender una amplia gama de intereses, tanto triviales como muy apremiantes, tanto claros como controvertidos. Así pues, será en una segunda fase, al tratar de sopesar dichos intereses en relación con los intereses y los derechos fundamentales de los afectados, cuando se deberá adoptar un enfoque más restringido y llevar a cabo un análisis más profundo.

La siguiente es una lista no exhaustiva de algunos de los contextos más comunes en los que puede surgir la cuestión del interés legítimo en el sentido del artículo 7, letra f). Se presenta a continuación sin perjuicio de si los intereses del responsable del tratamiento prevalecerán en

último término sobre los intereses y los derechos de los interesados cuando se realice la prueba de sopesamiento.

- el ejercicio del derecho de libertad de expresión o información, incluidas las situaciones en las que se ejerza dicho derecho en los medios de comunicación y en las artes;
- la prospección convencional y otras formas de comercialización o publicidad;
- los mensajes no comerciales que no hayan sido solicitados, incluidos los pertenecientes a campañas políticas o de recaudación de fondos para organizaciones caritativas;
- la ejecución de derechos reconocidos en procedimientos judiciales, incluido el cobro de deudas mediante procedimientos extrajudiciales;
- la prevención del fraude, el uso indebido de servicios o el blanqueo de dinero;
- la supervisión de los empleados con fines de seguridad o de gestión;
- los regímenes internos de denuncia de irregularidades;
- la seguridad física, la tecnología de la información y la seguridad en la red;
- el tratamiento con fines históricos, científicos o estadísticos;
- el tratamiento con fines de investigación (incluida la investigación de mercado).

Por consiguiente, un interés puede considerarse legítimo siempre que el responsable del tratamiento pueda perseguir este interés de conformidad con las leyes relativas a la protección de datos y con el resto de la legislación. En otras palabras, un interés legítimo debe ser «aceptable en virtud de la ley»[48].

Por tanto, un «interés legítimo» que sea pertinente en virtud del artículo 7, letra f), debe:

- ser lícito (es decir, de conformidad con la legislación nacional y de la UE aplicable);
- estar articulado con la claridad suficiente para permitir que la prueba de sopesamiento se lleve a cabo en contraposición a los intereses y los derechos fundamentales del interesado (es decir, suficientemente específico);
- representar un interés real y actual (es decir, no especulativo).

El hecho de que el responsable del tratamiento tenga dicho interés legítimo en el tratamiento de determinados datos no significa que pueda, necesariamente, utilizar el artículo 7, letra f), como fundamento jurídico del mismo. La legitimidad del interés del responsable del

[48] Las observaciones sobre la naturaleza de la «legitimidad» contenidas en la sección III.1.3 del Dictamen 3/2013 del Grupo de trabajo sobre la limitación de la finalidad (citado en el pie de página 9 anterior) también se aplican en este caso mutatis mutandis. Como reza en las páginas 19-20 de dicho Dictamen, el concepto de «ley» se utiliza en este caso en el sentido más amplio. Este comprende otras leyes aplicables como el Derecho laboral, contractual o en materia de protección de los consumidores. Además, la noción de «ley» comprende todas las formas de Derecho escrito y consuetudinario, la legislación primaria y secundaria, los decretos municipales, los precedentes judiciales, los principios constitucionales, los derechos fundamentales, otros principios jurídicos, así como la jurisprudencia, de modo que los tribunales competentes deberán interpretar dicha «ley» y tenerla en consideración. Dentro de los límites del Derecho, otros elementos como las costumbres, los códigos de conducta, los códigos deontológicos, las disposiciones contractuales, el contexto general y los hechos del caso pueden también considerarse al determinar si una finalidad concreta es legítima. Esto comprenderá la naturaleza de la relación subyacente entre el responsable del tratamiento y los interesados, ya sea comercial o de otro tipo. Por otro lado, aquello que puede considerarse un interés legítimo puede también cambiar con el tiempo, dependiendo de la evolución científica y tecnológica, y de los cambios que se producen en la sociedad y en las actitudes culturales.

tratamiento es solo un punto de partida, uno de los elementos que deben analizarse en virtud del artículo 7, letra f). Si el artículo 7, letra f), puede utilizarse como fundamento jurídico o no dependerá del resultado de la prueba de sopesamiento siguiente.

Sirva como ejemplo: los responsables del tratamiento pueden tener un interés legítimo en conocer las preferencias de sus clientes de manera que esto les permita personalizar mejor sus ofertas y, en último término, ofrecer productos y servicios que respondan mejor a las necesidades y los deseos de sus clientes. A la luz de esto, el artículo 7, letra f), puede constituir un fundamento jurídico apropiado en algunos tipos de actividades de mercado, en línea y fuera de línea, siempre que se prevean las garantías adecuadas (incluido, entre otros, un mecanismo viable que permita oponerse al tratamiento en virtud del artículo 14, letra b), tal como se explicará en la sección III.3.6 *El derecho de oposición y más allá*).

Sin embargo, esto no quiere decir que los responsables del tratamiento puedan remitirse al artículo 7, letra f), como fundamento jurídico para supervisar de manera indebida las actividades en línea y fuera de línea de sus clientes, combinar enormes cantidades de datos sobre ellos, provenientes de diferentes fuentes, que fueran inicialmente recopilados en otros contextos y con fines diferentes, y crear —y, por ejemplo, con la intermediación de corredores de datos, también comerciar con ellos— perfiles complejos de las personalidades y preferencias de los clientes sin su conocimiento, sin un mecanismo viable de oposición, por no mencionar la ausencia de un consentimiento informado. Es probable que dicha actividad de elaboración de perfiles represente una intrusión importante en la privacidad del cliente y, cuando esto suceda, los intereses y derechos del interesado prevalecerán sobre el interés del responsable del tratamiento[49].

Por poner otro ejemplo, en su Dictamen sobre SWIFT[50], aunque el Grupo de trabajo reconoció el legítimo interés de la empresa en cumplir las citaciones en virtud de la legislación estadounidense para evitar el riesgo de ser sancionada por las autoridades de EE.UU., concluyó que esta no podía remitirse al artículo 7, letra f), como fundamento jurídico. Más concretamente, el Grupo de trabajo consideró que, debido a los importes efectos de gran envergadura sobre las personas afectadas por un tratamiento de datos llevado a cabo de «forma oculta, sistemática, masiva y prolongada», «el interés o los derechos y libertades fundamentales de los numerosos interesados prevalece sobre el interés de SWIFT por no ser sancionado por los EE.UU. por posible incumplimiento de las citaciones».

Tal como se explicará a continuación, si el interés perseguido por el responsable del tratamiento no es apremiante, es más probable que el interés y los derechos del interesado prevalezcan sobre el interés legítimo —pero menos importante— del responsable del tratamiento. Del mismo modo, esto no significa que un interés menos apremiante del responsable del tratamiento no pueda prevalecer a veces sobre los intereses y derechos de los interesados: esto sucede normalmente cuando el impacto del tratamiento sobre los interesados es también menos importante.

---

49 La cuestión de las tecnologías de seguimiento y el papel que desempeña el consentimiento en virtud del artículo 5, apartado 3, de la Directiva sobre la intimidad en las comunicaciones electrónicas se debatirán aparte. Véase la sección III.3.6, letra b), bajo el epígrafe «Ejemplo: la evolución en el enfoque de la prospección ».

50 Véase la sección 4.2.3 del Dictamen ya citado en el pie de página 39 anterior. El interés legítimo del responsable del tratamiento en este caso estaba también vinculado al interés público de un tercer país, que no podía tener cabida en el ámbito de la Directiva 95/46/CE.

Interés legítimo del sector público

El texto actual de la Directiva no excluye específicamente a los responsables del tratamiento que sean autoridades públicas de la utilización del artículo 7, letra f), como fundamento jurídico del tratamiento de los datos[51].

Sin embargo, la propuesta de Reglamento[52] excluye esta posibilidad para el «tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones».

El cambio legislativo propuesto destaca la importancia del principio general de que las autoridades públicas, como norma, solo deberán tratar datos en el ejercicio de sus funciones en caso de que tengan autorización adecuada por ley para hacerlo. El cumplimiento de este principio es especialmente importante —y se exige claramente en la jurisprudencia del Tribunal Europeo de Derechos Humanos— en los casos en los que la privacidad de los interesados esté en juego y las actividades de la autoridad pública supongan una injerencia en dicha privacidad.

Por consiguiente, se requiere una autorización suficientemente *detallada y específica* por ley, también en virtud de la actual Directiva, en el caso de que el tratamiento por parte de las autoridades públicas suponga una injerencia en la privacidad de los interesados. Esto puede adoptar la forma de una obligación jurídica específica para el tratamiento de los datos que pueda ser conforme al artículo 7, letra c), o una autorización específica (aunque no necesariamente una obligación) para el tratamiento de los datos, que pueda cumplir los requisitos el artículo 7, letras e) o f)[53].

Interés legítimo de terceros

El texto actual de la Directiva no solo se refiere al «interés legítimo perseguido por el responsable del tratamiento», sino que también permite que el artículo 7, letra f), se utilice cuando dicho interés legítimo es perseguido por «el tercero o terceros a los que se comuniquen los datos»[54]. Los siguientes ejemplos ilustran algunos de los contextos en los que puede aplicarse esta disposición.

---

51 Originalmente, la primera propuesta de Directiva de la Comisión cubría el tratamiento de datos en el sector privado y las actividades de tratamiento del sector público por separado. Esta distinción formal entre las normas aplicables al sector público y al sector privado se suprimió en la propuesta modificada. Esto puede haber dado lugar también a diferencias en la interpretación y la aplicación por parte de los diversos Estados miembros.

52 Véase el artículo 6, apartado 1, letra f), de la propuesta de Reglamento.

53 En este sentido, véase también la sección III.2.5 anterior sobre misiones de interés público (páginas 25 a 28), así como los debates a continuación bajo el epígrafe Interés legítimo de terceros (páginas 32 a 34). Véanse también las reflexiones sobre los límites de la «aplicación en el ámbito privado» de la ley en la página 35 bajo el epígrafe «interés público/intereses de la comunidad en general». En todas estas situaciones, es especialmente importante garantizar que los límites del artículo 7, letras f) y e), se respetan plenamente.

54 La propuesta de Reglamento tiene como objetivo limitar el uso de este motivo para legitimar el interés perseguido por el responsable del tratamiento. No queda claro a partir únicamente del texto si el lenguaje propuesto significa una mera simplificación del mismo o si su intención es excluir situaciones en las que el responsable del tratamiento pudiera revelar datos en el interés legítimo de otros. No obstante, este texto no es definitivo. El interés de terceros se reintrodujo, por ejemplo, en el Informe final de la Comisión LIBE con motivo de las enmiendas acordadas por la Comisión LIBE del Parlamento Europeo el 21 de octubre de

Publicación de datos con fines de transparencia y responsabilidad. Un contexto importante en el que el artículo 7, letra f), puede ser pertinente es el caso de la publicación de los datos con fines de transparencia y responsabilidad (por ejemplo, los salarios de los altos cargos de una empresa). En este caso puede considerarse que la revelación pública se hace principalmente no en interés del responsable del tratamiento que publica los datos, sino en el interés de otras partes interesadas, tales como empleados, periodistas o el público general, a las que se comuniquen los datos.

Desde la perspectiva de la protección de datos y la privacidad, y para garantizar la seguridad jurídica, en general, es aconsejable que los datos personales se revelen al público de conformidad con una ley que permita y, cuando así proceda, claramente especifique los datos que deben publicarse, los fines de la publicación y cualesquiera garantías necesarias[55]. Esto también significa que puede ser preferible que se utilice el artículo 7, letra c), en lugar de la letra f), como base jurídica, cuando los datos personales se revelen con fines de transparencia y responsabilidad[56].

Sin embargo, en ausencia de una obligación o permiso jurídico específico para publicar los datos, sería posible, no obstante, revelar datos personales a las partes interesadas pertinentes. En los casos apropiados, sería también posible publicar datos personales con fines de transparencia y responsabilidad.

En ambos casos, es decir, independientemente de si los datos personales se revelan de conformidad con una ley que lo permita o no, la revelación depende directamente del resultado de la prueba de sopesamiento con arreglo al artículo 7, letra f), y de la aplicación de las medidas y garantías apropiadas[57].

Además, también puede ser deseable una reutilización de datos personales ya publicados para una mayor transparencia (por ejemplo, una nueva publicación de los datos por parte de la prensa o una mayor difusión de una serie de datos originalmente publicados de una manera más innovadora y simplificada por parte de una ONG). La posibilidad de dicha nueva publicación o reutilización también dependerá del resultado de la prueba de sopesamiento,

---

2013. Véase la enmienda 100 sobre el artículo 6. El Grupo de trabajo apoya la reintroducción de terceros en la Propuesta basándose en que su uso puede continuar siendo apropiado en algunas situaciones, incluidas las descritas a continuación.

55 Esta recomendación de mejores prácticas se hace sin perjuicio de las normas jurídicas nacionales en materia de transparencia y acceso del público a los documentos.

56 De hecho, en algunos Estados miembros deben cumplirse diferentes normas respecto del tratamiento llevado a cabo por partes públicas y privadas. Por ejemplo, de acuerdo con el Código de protección de datos italiano, la difusión de datos personales por un organismo público solo se permitirá si está estipulada por una ley o normativa (sección 19.3).

57 Tal como se explica en el Dictamen 06/2013 del Grupo de trabajo sobre datos abiertos (véase la página 10 de dicho Dictamen, citado más adelante en el pie de página 88), «la legislación nacional debe cumplir lo dispuesto en el artículo 8 del Convenio Europeo de Derechos Humanos (en lo sucesivo, «CEDH») y en los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea («Carta de la UE»). Esto implica, tal como sostuvo el Tribunal de Justicia en las sentencias Österreichischer Rundfunk y Schecke, que será necesario cerciorarse de que la divulgación sea necesaria y proporcionada al objetivo legítimo perseguido por la legislación. Véase la sentencia del TJUE de 20 de mayo de 2003, Rundfunk, en los asuntos acumulados C-465/00, C-138/01 y C-139/01 y la sentencia del TJUE de 9 de noviembre de 2010, Volker und Markus Schecke, en los asuntos acumulados C-92/09 y C-93/09.

que deberá tener en cuenta, entre otras cosas, la naturaleza de la información y el efecto de la nueva publicación o reutilización sobre las personas afectadas[58].

Investigación histórica u otro tipo de investigación científica. Otro contexto importante en el que la revelación en el interés legítimo de terceros puede ser pertinente es la investigación histórica u otros tipos de investigación científica, especialmente cuando se requiere el acceso a determinadas bases de datos. La Directiva prevé el reconocimiento específico de dichas actividades, sujetas a las garantías y medidas adecuadas[59], pero no debe olvidarse que el fundamento jurídico de estas actividades será con frecuencia un uso bien evaluado del artículo 7, letra f)[60].

Interés público general o interés de un tercero. Por último, el interés legítimo de terceros puede ser pertinente también de un modo diferente. Se trata del caso en el que el responsable del tratamiento, a veces instado por las autoridades públicas, persigue un interés que se corresponde con un interés público general o el interés de un tercero. Esto puede comprender situaciones en las que el responsable del tratamiento vaya más allá de sus obligaciones jurídicas específicas establecidas en las leyes y reglamentos para facilitar la aplicación de la legislación o para ayudar a las partes interesadas privadas en sus esfuerzos por combatir las actividades ilegales, tales como el blanqueo de dinero, la captación de menores o el intercambio ilegal de archivos en línea. En estas situaciones, no obstante, es especialmente importante garantizar que los límites del artículo 7, letra f), se respetan plenamente[61].

El tratamiento debe ser necesario para el fin o los fines previstos

Finalmente, el tratamiento de datos personales debe ser también «necesario para la satisfacción del interés legítimo» perseguido por el responsable del tratamiento o, en el caso de revelación de los datos, por la tercera parte. Esta condición complementa el requisito de necesidad en virtud del artículo 6 y exige una relación entre el tratamiento y el interés perseguido. Este requisito de «necesidad» se aplica a todas las situaciones mencionadas en el artículo 7, letras b) a f), pero es especialmente pertinente en el caso de la letra f) con el fin de garantizar que el tratamiento de los datos basado en el interés legítimo no dé lugar a una interpretación indebidamente amplia de la necesidad de tratar los datos. Como en otros casos,

---

58 La limitación de la finalidad es también una consideración importante en este caso. En la página 21 del Dictamen 06/2013 del Grupo de trabajo sobre datos abiertos (citado más adelante, en el pie de página 88), el Grupo de trabajo del artículo 29 recomienda «que toda legislación que prevea el acceso público a la información especifique claramente la finalidad de la divulgación de los datos personales. Si esto no se hace, o se hace en términos vagos y generales, se verán perjudicadas la seguridad y la previsibilidad jurídicas. En particular, por lo que respecta a las solicitudes de reutilización, será muy difícil para el organismo del sector público y para los reutilizadores potenciales determinar cuáles fueron los fines inicialmente previstos de la publicación y, posteriormente, qué otros fines serían compatibles con estos. Como ya se ha mencionado, incluso si los datos personales se publican en Internet, no debe suponerse que pueden ser tratados para cualquier fin posible».

59 Véase, por ejemplo, el artículo 6, apartado 1, letras b) y e).

60 Tal como se explica en el Dictamen 3/2013 del Grupo de trabajo sobre la limitación de la finalidad (citado en el pie de página 9 anterior), una reutilización de los datos con fines secundarios deberá cumplir una condición doble: en primer lugar, deberá garantizar que los datos se utilizarán con fines compatibles; en segundo lugar, deberá garantizar que exista una base jurídica apropiada para el tratamiento en virtud del artículo 7.

61 Véase en este sentido, por ejemplo, el Documento de trabajo sobre cuestiones relativas a la protección de datos relacionadas con los derechos de propiedad intelectual, aprobado el 18 de enero de 2005 (WP 104).

esto significa que deberá considerarse si se dispone de otros medios menos invasivos para servir al mismo fin.

III.3.2. Intereses o derechos del interesado

Intereses o derechos (en vez de intereses en materia de derechos)

El artículo 7, letra f), de la Directiva se refiere a «los intereses en materia de derechos y libertades fundamentales del interesado que requieran protección en virtud del artículo 1, apartado 1».

Sin embargo, el Grupo de trabajo ha advertido, al comparar las diferentes versiones lingüísticas de la Directiva que la frase «intereses en materia de» se ha traducido como «intereses o» en otras lenguas clave utilizadas cuando se negoció el texto[62].

Un análisis más detallado sugiere que el texto en inglés de la Directiva es simplemente el resultado de un error tipográfico: «*or*» («o») se escribió erróneamente como «*for*» («en materia de»)[63]. Por tanto, el texto correcto deberá leerse «intereses o derechos y libertades fundamentales».

Los términos «intereses» y «derechos» deberán interpretarse en sentido amplio

La referencia a los «intereses o derechos y libertades fundamentales» tiene una repercusión directa en el ámbito de aplicación de esta disposición. Prevé más protección al interesado, es decir, exige que se tenga en cuenta también el «interés» de los afectados, no solo sus derechos y libertades fundamentales. No obstante, no hay motivo para suponer que la restricción del artículo 7, letra f), a los derechos fundamentales «que requieran protección en virtud del apartado 1 del artículo 1» —y, por tanto, la referencia explícita al objeto de la Directiva[64]— no se deba aplicar también al término «intereses». En cualquier caso, el mensaje es claro: deben tenerse en cuenta todos los intereses pertinentes del interesado.

Esta interpretación del texto tiene sentido no solo gramaticalmente, sino también teniendo en consideración la interpretación en sentido amplio del concepto de «interés legítimo» del responsable del tratamiento. Si el responsable del tratamiento —o el tercero en el caso de

---

62 Por ejemplo, «l'intérêt ou les droits et libertés fondamentaux de la personne concernée» en francés; «l'interesse o i diritti e le libertà fondamentali della persona interessata» en italiano; «das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person» en alemán.

63 El Grupo de trabajo advierte que la versión inglesa gramaticalmente correcta debería rezar: «intereses en» en vez de «intereses en materia de», si esto es lo que quería expresarse. Además, la frase «intereses en materia de» o «intereses en» parece redundante, en primer término, porque la referencia a los «derechos y libertades fundamentales» debería bastar normalmente, si esto es lo que se pretendía expresar. La interpretación de que se ha producido un error tipográfico también se confirma por el hecho de que la Posición común (CE) nº 1/1995 del Consejo de 20 de febrero de 1995 también hace referencia a los «intereses o derechos y libertades fundamentales» y no «intereses en materia de» dichos derechos. Por último, el Grupo de trabajo también advierte que la Comisión ha intentado corregir dicho error tipográfico en la propuesta de Reglamento: El artículo 6, apartado 1, letra f) se refiere a «los intereses o los derechos y libertades fundamentales del interesado que requieran protección de los datos personales» y no a los «intereses en materia de» dichos derechos.

64 Véase el artículo 1, apartado 1: «Los Estados miembros garantizarán, con arreglo a las disposiciones de la presente Directiva, la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales».

revelación— puede perseguir cualquier interés, siempre que no sea ilegítimo, entonces el interesado deberá también tener derecho a que se tengan en cuenta todas las categorías de intereses que le afecten y a que se ponderen en relación con los intereses del responsable del tratamiento, en tanto en cuanto estén comprendidos en el ámbito de la Directiva.

En un momento de creciente desequilibrio en el «poder de la información», cuando tanto los gobiernos como las organizaciones empresariales manejan cantidades de datos personales sin precedentes hasta ahora, y se encuentran cada vez más en una posición de compilar perfiles detallados que puedan predecir el comportamiento (reforzando el desequilibrio informativo y reduciendo la autonomía), resulta especialmente importante garantizar que se protege el derecho de las personas a preservar su privacidad y su autonomía.

Por último, es importante destacar que, a diferencia del caso de los intereses del responsable del tratamiento, el adjetivo «legítimo» no precede aquí al término «intereses» de los interesados. Esto implica un ámbito más amplio de protección de los intereses y derechos de las personas. Incluso las personas implicadas en actividades ilegales no deberán estar sujetas a una injerencia desproporcionada en sus derechos e intereses[65]. Por ejemplo, los intereses de una persona que pueda haber cometido un robo en un supermercado deberán prevalecer sobre la publicación de su foto y su dirección privada en las paredes del supermercado o en Internet por parte del propietario de la tienda.

III.3.3. Introducción a la aplicación de la prueba de sopesamiento

Resulta útil imaginar tanto el interés legítimo del responsable del tratamiento como el impacto sobre los intereses y derechos del interesado en un espectro. El interés legítimo puede variar de insignificante a ligeramente importante, hasta llegar a apremiante. De igual modo, la repercusión en los intereses y los derechos de los interesados puede ser más o menos importante y puede variar de trivial a muy grave.

El interés legítimo del responsable del tratamiento, cuando es menor y no muy apremiante, en general, solo anula los intereses y los derechos de los interesados en casos en los que el impacto sobre estos derechos e intereses sea incluso más trivial. Por otro lado, un interés legítimo importante y apremiante puede, en algunos casos y sujeto a garantías y medidas, justificar incluso una intrusión significativa en la privacidad o cualquier otra repercusión importante en los intereses o derechos de los interesados[66].

---

65 Por supuesto, una de las consecuencias de la delincuencia puede ser la recopilación y posible publicación de datos personales sobre delincuentes y sospechosos. No obstante, esto debe estar sujeto a condiciones y garantías estrictas.

66 Véase como ejemplo el razonamiento del Grupo de trabajo en varios dictámenes y documentos de trabajo:
- Dictamen 4/2006 sobre la notificación de la propuesta de Reglamento por parte del «US Departament of Health and Human Services», de 20 de noviembre de 2005, relativo al control de las enfermedades contagiosas y a la obtención de información sobre pasajeros (Control de las enfermedades contagiosas, Propuesta CFR 42, partes 70 y 71), adoptado el 14 de junio de 2006 (WP 121), en los casos en los que existen graves amenazas concretas para la salud pública.
- Dictamen 1/2006 relativo a los sistemas internos de denuncia de irregularidades (citado anteriormente en el pie de página 39), cuando la gravedad de un supuesto delito es uno de los elementos de la prueba de sopesamiento.
- Documento de trabajo relativo a la vigilancia de las comunicaciones electrónicas en el lugar de trabajo, aprobado el 29 de mayo de 2002 (WP 55), que pondera el derecho del empleador a administrar con cierta eficacia la empresa en relación con la dignidad humana del trabajador, así como el secreto de la correspondencia.

Aquí es importante destacar el papel especial que las garantías pueden desempeñar[67] para reducir un impacto indebido sobre los interesados y, por tanto, para cambiar el equilibrio de derechos e intereses hasta el punto de que prevalezca el interés legítimo del responsable del tratamiento de datos. Por supuesto, el uso de garantías exclusivamente no es suficiente para justificar cualquier tipo de tratamiento en cualquier contexto. Además, las garantías en cuestión deben ser adecuadas y suficientes, y deben, incuestionable y significativamente, reducir la repercusión para los interesados.

Escenarios introductorios

Antes de avanzar en la elaboración de directrices sobre el modo de efectuar la prueba de sopesamiento, los siguientes tres escenarios introductorios pueden proporcionar un primer ejemplo de cómo ponderar intereses y derechos en la vida real. Los tres ejemplos se basan en un escenario sencillo e inocente que comienza con una oferta especial de comida italiana para llevar. Los ejemplos introducen de manera gradual elementos nuevos que ponen de manifiesto cómo se inclina la balanza según aumenta el impacto sobre los interesados.

Escenario 1: Oferta especial por una cadena de pizzerías

Claudia ordena una pizza mediante una aplicación móvil en su teléfono inteligente, pero no se excluye voluntariamente de la publicidad en el sitio web. Su dirección y los datos de su tarjeta de crédito se almacenan para la entrega del producto. Unos días más tarde Claudia recibe cupones de descuento para productos similares de la cadena de pizzerías en el buzón de correos de su casa.

Breve análisis: La cadena de pizzerías tiene un interés legítimo, aunque no especialmente apremiante, en intentar vender más productos a sus clientes. Por otro lado, no parece que haya una intrusión significativa en la privacidad de Claudia, ni ninguna otra repercusión indebida en sus intereses y derechos. Los datos y el contexto son relativamente inocentes (consumo de pizza). La cadena de pizzerías estableció ciertas garantías: solo se utiliza información relativamente limitada (datos de contacto) y los cupones se envían por correo tradicional. Además, se ofrece una posibilidad, fácil de usar, de exclusión voluntaria de la publicidad en el sitio web.

En conjunto, y considerando también las garantías y medidas previstas (incluida la opción de exclusión voluntaria fácil de usar), no parece que los intereses y derechos del interesado prevalezcan sobre el interés legítimo de la cadena de pizzerías de realizar esta cantidad mínima de tratamiento de datos.

[67] Las garantías podrán comprender, entre otras, unas limitaciones estrictas sobre la cantidad de datos que se recopilen, la eliminación inmediata de los datos después de su utilización, medidas técnicas y organizativas para garantizar la separación funcional, el uso apropiado de técnicas de anonimización, la agregación de datos y las tecnologías de protección de la intimidad, pero también mayor transparencia, responsabilidad y la posibilidad de exclusión voluntaria del tratamiento. Véanse más detalles en la sección III.3.4, d) y en otras partes .

Escenario 2: Publicidad dirigida para la misma oferta especial

El contexto es el mismo, pero esta vez la cadena de pizzerías no solo almacena la dirección y los datos de la tarjeta de crédito de Claudia sino también su historial de pedidos reciente (durante los últimos tres años). Además, el historial de compras se combina con datos del supermercado en el que Claudia hace sus compras en línea, que está gestionado por la misma empresa que gestiona la cadena de pizzerías. La cadena de pizzerías ofrece a Claudia ofertas especiales y publicidad dirigida basada en su historial de pedidos de los dos diferentes servicios. Recibe anuncios y ofertas especiales tanto en línea como fuera de línea, por correo ordinario, correo electrónico y publicación en el sitio web de la empresa, así como en el sitio web de una serie de socios seleccionados (cuando ella accede a estos sitios en su ordenador o mediante su teléfono móvil). También se hace un seguimiento de su historial de navegación (recorrido por Internet) y de sus datos de localización mediante su teléfono móvil. Se utiliza un software para analizar los datos, que predice sus preferencias y los momentos y ubicaciones en los que es más probable que realice una compra mayor, dispuesta a pagar un precio más elevado, susceptible de ser influida por un determinado tipo de descuento, o cuándo desea más sus comidas preparadas o postres favoritos[68]. Claudia está realmente molesta por los persistentes anuncios que aparecen en su teléfono móvil cuando comprueba los horarios de los autobuses camino a casa, con las últimas ofertas de comida para llevar a las que trata de resistirse. No puede encontrar información fácil de usar o un modo sencillo de suprimir estos anuncios, aunque la empresa afirma que cuenta con un sistema de exclusión voluntaria en el conjunto del sector. También se ve sorprendida al comprobar que cuando se traslada a una vecindad menos favorecido deja de recibir sus ofertas especiales. Esto da lugar a un aumento de aproximadamente el 10 % de su factura mensual de comida. Un amigo aficionado a la tecnología le muestra algunos comentarios en un blog en línea en los que se especula que el supermercado está cobrando más por los pedidos a las «vecindades peores» basándose en un riesgo estadístico mayor de fraude de las tarjetas de crédito en dichos casos. La empresa no hace comentarios y afirma que su política sobre descuentos y el algoritmo que utiliza para fijar los precios son privados y no pueden revelarse.

Breve análisis: los datos y el contexto siguen teniendo un carácter relativamente inocente. Sin embargo, la escala de la recopilación de datos y las técnicas utilizadas para influir en Claudia (incluidas varias técnicas de seguimiento y predicción de las ubicaciones y los momentos en los que pueda desear comida y el hecho de que en esos momentos Claudia sea más vulnerable a sucumbir a la tentación), son factores que deben considerarse cuando se evalúe la repercusión del tratamiento. La falta de transparencia sobre la lógica del tratamiento de datos de la empresa, que puede llevar a una discriminación de precios *de facto* basada en la ubicación de donde procede el pedido, y la significativa repercusión potencial financiera para los clientes en última instancia inclinan la balanza, incluso en el contexto relativamente inocente de comida para llevar y compra de alimentos. En vez de ofrecer solamente la posibilidad de exclusión voluntaria de este tipo de publicidad dirigida y personalizada, sería necesario un consentimiento informado de conformidad con el artículo 7, letra a) y también en virtud del artículo 5, apartado 3, de la Directiva sobre intimidad y comunicaciones electrónicas. Como consecuencia de ello, el artículo 7, letra f), no deberá utilizarse como fundamento jurídico del tratamiento.

[68] Véase, por ejemplo, http://www.stanfordlawreview.org/online/privacy-and-big-data/consumer-subject-review-boards: Los estudios recientes sugieren que la voluntad es un recurso finito que puede agotarse o

Escenario 3: Uso de los datos sobre pedidos de comida para adaptar las primas del seguro de enfermedad

La cadena vende los datos sobre los hábitos de consumo de pizza de Claudia, incluidos el momento y la naturaleza de los pedidos de comida, a una empresa de seguros, que los utiliza para adaptar sus primas del seguro de enfermedad.

Breve análisis: La empresa de seguros de enfermedad puede tener un interés legítimo, en la medida en que la normativa aplicable lo permita, en evaluar los riesgos sanitarios de sus clientes y en cobrarles primas diferenciadas según sus diversos riesgos. Sin embargo, la manera en la que se recopilan los datos y la escala de la recopilación de datos son en sí mismas excesivas. Resulta improbable que una persona en la situación de Claudia espere razonablemente que la información sobre su consumo de pizza se utilice para calcular las primas de su seguro de enfermedad.

Además del carácter excesivo de la elaboración de perfiles y de las posibles injerencias inapropiadas (la pizza podría pedirse para otra persona), la injerencia en datos sensibles (datos relativos a la salud) a partir de datos aparentemente inocuos (pedidos para llevar) contribuye a inclinar la balanza a favor de los intereses y derechos del interesado. Por último, el tratamiento también tiene una repercusión financiera importante para ella.

En conjunto, en este caso concreto los intereses y derechos del interesado prevalecen sobre el interés legítimo de la compañía de seguros sanitarios. Como consecuencia, el artículo 7, letra f), no deberá utilizarse como fundamento jurídico del tratamiento. También es cuestionable si el artículo 7, letra a), podría utilizarse como fundamento jurídico, teniendo en consideración la escala excesiva de la recopilación de datos y, posiblemente, también debido a restricciones adicionales específicas en virtud de la legislación nacional.

Los anteriores escenarios y la posible introducción de variaciones debido a otros elementos ponen de manifiesto la necesidad de definir un número limitado de factores clave que puedan ayudar a centrar la evaluación, así como la necesidad de un enfoque pragmático que permita la utilización de supuestos prácticos («reglas generales») basados, en primer lugar, en lo que una persona consideraría razonablemente aceptable en virtud de las circunstancias («expectativas razonables») y, en segundo lugar, en las consecuencias de la actividad de tratamiento de los datos para los interesados («repercusiones»).

III.3.4. Factores clave que deben considerarse al efectuar la prueba de sopesamiento

Los Estados miembros han definido una serie de factores útiles que deben considerarse al efectuar la prueba de sopesamiento. Estos factores se debaten en esta sección bajo los siguientes cuatro epígrafes principales: a) evaluación del interés legítimo del responsable del tratamiento; b) impacto sobre los interesados; c) equilibrio provisional y d) garantías

reponerse en el tiempo.[10] Imaginemos que las inquietudes sobre la obesidad llevan a un consumidor a tratar de vetar su comida basura favorita, pero hay momentos y lugares en los que no puede. Los macrodatos pueden ayudar a los publicistas a comprender exactamente cómo y cuándo abordar a este consumidor en su momento más vulnerable, especialmente en un mundo de pantallas constantes en el que incluso nuestras aplicaciones pueden desarrollar una estrategia de venta.

adicionales aplicadas por el responsable del tratamiento para impedir cualquier impacto indebido sobre los interesados[69].

Con el fin de llevar a cabo la prueba de sopesamiento, es importante considerar, en primer lugar, la naturaleza y la fuente del interés legítimo, por un lado, y las repercusiones para los interesados, por otro. Esta evaluación deberá ya tener en cuenta las medidas que el responsable del tratamiento se propone adoptar para cumplir con la Directiva (por ejemplo, con el fin de garantizar la limitación de la finalidad y la proporcionalidad en virtud del artículo 6, o para facilitar información a los interesados conforme a los artículos 10 y 11).

Después de analizar y sopesar los dos lados de la balanza, puede establecerse un «equilibrio» provisional. Cuando el resultado de la evaluación deje todavía lugar a dudas, el siguiente paso será evaluar si unas garantías adicionales que ofrezcan más protección al interesado pueden inclinar la balanza de modo que se legitime el tratamiento.

a) Evaluación del interés legítimo del responsable del tratamiento

Aunque el concepto de interés legítimo es bastante amplio, tal como se explica en la sección III.3.1 anterior, esta noción desempeña un papel crucial a la hora de sopesar el interés del responsable en relación con los derechos y los intereses de los afectados. A pesar de que es imposible hacer juicios de valor respecto de todos los intereses legítimos potenciales, sí es posible facilitar algunas directrices. Tal como se afirma anteriormente, dicho interés puede variar desde trivial hasta apremiante, y puede ser claro o más controvertido.

i) Ejercicio de un derecho fundamental

Entre los derechos y libertades fundamentales consagrados en la Carta de los Derechos Fundamentales de la Unión Europea (la «Carta»)[70] y el Convenio Europeo de Derechos Humanos («CEDH»), varios de esos derechos pueden entrar en conflicto con el derecho a la intimidad y el derecho a la protección de los datos personales, como la libertad de expresión y de información[71], la libertad de las artes y de las ciencias[72], el derecho de acceso a los documentos[73], así como, por ejemplo, el derecho a la libertad y a la seguridad[74], la libertad de pensamiento, de conciencia y de religión[75], la libertad de empresa[76], el derecho a la

69 Debido a su importancia, algunas cuestiones concretas relacionadas con las garantías se debatirán más extensamente bajo epígrafes separados en las secciones III.3.5 y III.3.6.

70 Las disposiciones de la Carta están dirigidas a las instituciones y los organismos de la UE con la debida consideración del principio de subsidiariedad y a las autoridades nacionales solo cuando éstas aplican la legislación de la UE.

71 Artículo 11 de la Carta y artículo 10 del CEDH.

72 Artículo 13 de la Carta y artículos 9 y 10 del CEDH.

73 Artículo 42 de la Carta. «Todo ciudadano de la Unión o toda persona física o jurídica que resida o tenga su domicilio social en un Estado miembro tiene derecho a acceder a los documentos del Parlamento Europeo, del Consejo y de la Comisión». Existe un derecho de acceso similar en una serie de Estados miembros en relación con los documentos en poder de los organismos del sector público de dichos Estados miembros.

74 Artículo 6 de la Carta y artículo 5 del CEDH.

75 Artículo 10 de la Carta y artículo 9 del CEDH.

76 Artículo 16 de la Carta.

propiedad[77], el derecho a la tutela judicial efectiva y a un juez imparcial[78], o la presunción de inocencia y derechos de la defensa[79].

Para que prevalezca el interés legítimo del responsable del tratamiento, el tratamiento de datos debe ser «necesario» y «proporcionado» con el fin de ejercer el derecho fundamental en cuestión.

Sirva como ejemplo que, dependiendo de los hechos del caso, puede resultar necesario y proporcionado que un periódico publique determinados datos incriminatorios sobre los hábitos de gasto de un alto cargo gubernamental implicado en un supuesto escándalo de corrupción. Por otro lado, no deberá existir una autorización general para que los medios publiquen cualquier dato irrelevante de la vida privada de las personalidades públicas. Estos y otros casos similares normalmente plantean complejas cuestiones de valoración y, con el fin de orientar la evaluación, la legislación específica, la doctrina legal, la jurisprudencia, las directrices, así como los códigos de conducta y otras normas formales o informales pueden desempeñar un papel fundamental[80].

Cuando así proceda, en este contexto igualmente, las garantías adicionales pueden también desempeñar un papel fundamental para ayudar a alcanzar un equilibrio a veces frágil.

ii) El interés público o el interés de la comunidad en general.

En algunos casos, el responsable del tratamiento puede desear invocar el interés público o el interés de la comunidad en general (tanto si esto está estipulado como si no en las leyes o normativas nacionales). Por ejemplo, una organización caritativa puede tratar datos personales con fines de investigación médica, o una organización sin ánimo de lucro con el fin de sensibilizar sobre la corrupción gubernamental.

Puede darse también el caso de que el interés privado de una empresa coincida con un interés público hasta cierto punto. Esto puede suceder, por ejemplo, respecto de la lucha contra el fraude financiero u otro uso fraudulento de servicios[81]. Un proveedor de servicios puede tener un interés empresarial legítimo en garantizar que sus clientes no hagan un mal uso del servicio (o no puedan obtener servicios sin el pago correspondiente), mientras que, al mismo tiempo, los clientes de la empresa, como contribuyentes, y el público en general también tengan un interés legítimo en garantizar que se desaliente la comisión de actividades fraudulentas y que se detecten cuando estas ocurran.

---

77 Artículo 17 de la Carta y artículo 1 del protocolo nº 1 del CEDH.

78 Artículo 47 de la Carta y artículo 6 del CEDH.

79 Artículo 48 de la Carta y artículos 6 y 13 del CEDH.

80 En relación con los criterios que se deben aplicar en casos relativos a la libertad de expresión, la jurisprudencia del Tribunal Europeo de Derechos Humanos también ofrece directrices útiles. Véase, por ejemplo, la sentencia del TEDH en el asunto von Hannover / Alemania (Nº 2) de 7 de febrero de 2012, en especial los apartados de 95 a 126. Debe también considerarse que el artículo 9 de la Directiva (bajo el título Tratamiento de datos personales y libertad de expresión) permite a los Estados miembros «establecer exenciones y excepciones [respecto de determinadas disposiciones de la Directiva], en lo referente al tratamiento de datos personales con fines exclusivamente periodísticos o de expresión artística o literaria», «sólo en la medida en que resulten necesarias para conciliar el derecho a la intimidad con las normas que rigen la libertad de expresión».

81 Véase, a título ilustrativo, el Ejemplo 21: Datos extraídos de contadores inteligentes para detectar el uso fraudulento de la energía en la página 67 del Dictamen 3/2013 del Grupo de trabajo sobre la limitación de la finalidad (citado en el pie de página 9 anterior).

En general, el hecho de que el responsable del tratamiento actúe no solo en su interés legítimo propio (por ejemplo, su empresa), sino también en el interés de la comunidad en general puede dar más «peso» a su interés. Cuanto más apremiante sea el interés público o el interés de la comunidad en general, y cuanto más claramente la comunidad y los interesados reconozcan y esperen que el responsable del tratamiento pueda actuar y tratar los datos para perseguir estos intereses, más peso tendrá en la balanza dicho interés legítimo.

Por otro lado, «el cumplimiento privado» de la ley no deberá utilizarse para legitimar prácticas intrusivas que estarían prohibidas, si las llevara a cabo una organización gubernamental, en virtud de la jurisprudencia del Tribunal Europeo de Derechos Humanos basándose en que dichas actividades por parte de la autoridad pública suponen una injerencia en la privacidad de los interesados al no pasar el riguroso filtro del apartado 2 del artículo 8 del CEDH.

iii) Otros intereses legítimos

En algunos casos, tal como se ha debatido ya en la sección III.2, el contexto en el que surge un interés legítimo puede ser parecido a uno de los contextos en los que pueden ser de aplicación algunos de los demás motivos de legitimación, en especial, los motivos de legitimación del artículo 7, letra b) (contrato), del artículo 7, letra c) (obligación jurídica) o del artículo 7, letra e) (misión de interés público). Por ejemplo, una actividad de tratamiento de datos puede no ser estrictamente necesaria, pero puede seguir siendo pertinente para la ejecución de un contrato, o una ley puede solo permitir que se traten determinados datos, pero no exigir su tratamiento. Tal como hemos visto, puede que no siempre resulte fácil trazar una línea divisoria clara entre los diferentes fundamentos, pero esto no hace sino corroborar la importancia de analizar la prueba de sopesamiento con arreglo al artículo 7, letra f).

En este caso, como en todos los demás casos posibles no mencionados hasta ahora, cuanto más apremiante sea el interés del responsable del tratamiento, y cuanto más claramente la comunidad en general reconozca y espere que el responsable del tratamiento pueda actuar y tratar los datos en la búsqueda de dicho interés, más peso tendrá en la balanza este interés legítimo[82]. Esto nos lleva al punto siguiente, más general.

iv) Reconocimiento jurídico y cultural o social de la legitimidad de los intereses

En todos los contextos anteriores también es, sin duda alguna, pertinente si la legislación de la UE o la legislación de un Estado miembro permite de manera específica (incluso aunque no lo exija) que los responsables del tratamiento adopten medidas para perseguir el interés público o privado en cuestión. La existencia de cualquier directriz no vinculante debidamente adoptada, emitida por los órganos competentes, por ejemplo, por las agencias reguladoras, instando a los responsables a tratar los datos en la búsqueda del interés en cuestión también resulta pertinente.

El cumplimiento de cualquier directriz no vinculante dictada por las autoridades de protección de datos u otros órganos competentes en relación con las modalidades del tratamiento de

[82] Por supuesto, la evaluación debe también incluir una reflexión sobre el posible perjuicio que el responsable del tratamiento, los terceros o la comunidad en general puedan sufrir si no se realiza el tratamiento de datos.

datos también es probable que contribuya a una valoración favorable del equilibrio. Las expectativas culturales y sociales, incluso cuando no se reflejen directamente en los instrumentos legislativos o normativos, también pueden desempeñar un papel y pueden ayudar a inclinar la balanza hacia cualquiera de los dos lados.

Cuanto más explícitamente reconocido se encuentre en la ley, en otros instrumentos normativos —sean vinculantes o no para el responsable del tratamiento— o incluso en la cultura de una comunidad determinada en general sin ninguna base jurídica específica, que los responsables del tratamiento puedan actuar y tratar los datos en la búsqueda de un interés específico, más peso tendrá en la balanza dicho interés legítimo[83].

b) Impacto sobre los interesados

Si se considera el otro lado de la balanza, la repercusión del tratamiento en los intereses o derechos y libertades fundamentales del interesado es un criterio crucial. En la primera subsección a continuación se debate en términos generales cómo evaluar el impacto sobre el interesado.

Varios elementos que pueden resultar útiles en este caso se analizan en las subsecciones siguientes, incluida la naturaleza de los datos personales, la manera en que se trata la información, las expectativas razonables de los interesados, y la posición del responsable del tratamiento y del interesado. También se debatirán brevemente cuestiones relativas a las fuentes potenciales de riesgo que puedan dar lugar a repercusiones para las personas implicadas, la gravedad de estas, y la probabilidad de que dichas repercusiones se materialicen.

[83] Este interés, no obstante, no se podrá utilizar para legitimar prácticas intrusivas que no pasarían de otro modo el filtro del artículo 8, apartado 2, del CEDH.

i) Evaluación del impacto

Al evaluar el impacto[84] del tratamiento, deberán tenerse en consideración las consecuencias tanto positivas como negativas. Estas podrán comprender futuras acciones o decisiones potenciales llevadas a cabo o tomadas por terceros, y situaciones en las que el tratamiento pueda dar lugar a la exclusión de personas o a su discriminación, difamación, o más en general, a situaciones en la que haya riesgo de daño a la reputación, al poder de negociación o a la autonomía del interesado.

Además de los resultados adversos que puedan preverse de manera específica, también deben tenerse en consideración las repercusiones emocionales más generales, como el enfado, el miedo y la angustia que puedan derivarse de la pérdida de control sobre la información personal por parte del interesado o del conocimiento de que dicha información personal ha sido o pueda ser mal utilizada o se vea comprometida, por ejemplo, mediante su exposición en Internet. El efecto amedrentador sobre el comportamiento protegido, como la libertad de investigación o la libertad de expresión, que pueda resultar de una supervisión o un seguimiento continuo también deberá tenerse en cuenta.

El Grupo de trabajo pone de manifiesto que es crucial entender que «impacto» pertinente es un concepto mucho más amplio que daño o perjuicio a uno o más interesados en concreto. El término «impacto» tal como se utiliza en este Dictamen cubre cualquier posible consecuencia (potencial o real) del tratamiento de datos. En aras de la claridad, también subrayamos que el concepto no está relacionado con la noción de violación de los datos personales y es mucho más amplio que las repercusiones que puedan derivarse de dicha violación. Por el contrario, la noción de impacto, tal como se utiliza aquí, engloba las diversas maneras en las que un individuo pueda verse afectado, positiva o negativamente, por el tratamiento de sus datos personales[85].

También es importante entender que, por lo general, una serie de situaciones relacionadas y no relacionadas pueden dar lugar acumulativamente a un impacto último negativo sobre el interesado y puede ser difícil identificar qué actividad de tratamiento por parte de qué responsable del tratamiento desempeñó un papel clave en el impacto negativo.

---

84 Esta evaluación de impacto puede entenderse en el contexto del artículo 7, letra f). En otras palabras, no nos referimos a un «análisis de riesgos» o a una «evaluación de impacto relativa a la protección de datos» en el sentido de la propuesta de Reglamento (artículos 33 y 34) y las diversas enmiendas de la Comisión LIBE a la misma. La cuestión de qué metodología deberá seguirse en un «análisis de riesgos» o una «evaluación de impacto relativa a la protección de datos» excede el ámbito de este Dictamen. Por otro lado, deberá tenerse en cuenta que, de un modo u otro, el análisis de impacto en virtud del artículo 7, letra f), puede ser una parte importante de cualquier «evaluación de riesgos» o «evaluación de impacto relativa a la protección de datos» y puede también ayudar a detectar situaciones en las que se deba consultar a la autoridad de protección de datos.

85 El riesgo de perjuicio financiero, por ejemplo, si una violación de los datos personales revela información financiera que supuestamente estaba guardada en un entorno seguro, y esto permite, en su caso, establecer la existencia de un robo u otras formas de fraude, o el riesgo de lesiones corporales, daños físicos, daños morales y pérdida de comodidades, que puedan, en su caso, derivarse de, por ejemplo, una alteración no autorizada de los registros médicos y un tratamiento indebido de un paciente, deben siempre tenerse en consideración, aunque no se limiten en modo alguno a situaciones en el ámbito del artículo 7, letra f). Al mismo tiempo, dichos riesgos no deberán ser los únicos que se deba tener en cuenta al evaluar el impacto en virtud del artículo 7, letra f).

Teniendo en cuenta que el establecimiento de una indemnización en un caso por un daño o perjuicio sufrido es, con frecuencia, difícil para los interesados en este contexto, incluso cuando el efecto en sí mismo es muy real, resulta especialmente importante centrarse en la prevención y garantizar que las actividades de tratamiento de datos puedan solo llevarse a cabo siempre que no conlleven riesgo o un riesgo muy bajo de impacto negativo indebido sobre los intereses o los derechos y libertades fundamentales de los afectados.

Al evaluar el impacto, la terminología y la metodología de la evaluación de riesgos tradicional pueden ser útiles en cierta medida y, por tanto, algunos elementos de esta metodología se destacan a continuación. No obstante, una metodología global de la evaluación del impacto, en el contexto del artículo 7, letra f), o más en general, excedería el ámbito del presente Dictamen.

En este contexto, como en los demás, es importante detectar las fuentes de repercusiones potenciales para los interesados.

La probabilidad de que un riesgo pueda materializarse es uno de los elementos que se ha de tener en cuenta. Por ejemplo, el acceso a Internet, el intercambio de datos con sitios fuera de la UE, las interconexiones con otros sistemas y el alto grado de heterogeneidad o variabilidad del sistema representan vulnerabilidades que los piratas informáticos podrían explotar. La fuente de riesgo conlleva una probabilidad relativamente alta de que se materialice el riesgo de comprometer la seguridad de los datos. Por el contrario, un sistema estable y homogéneo que no tenga interconexiones y esté desconectado de Internet conlleva una probabilidad mucho menor de poner en peligro la seguridad de los datos.

Otro elemento de la evaluación del riesgo es la gravedad de las consecuencias de un riesgo que se haya materializado. Esta gravedad puede variar desde niveles bajos (como la molesta necesidad de introducir de nuevo los datos personales de contacto perdidos por el responsable del tratamiento de los datos) a niveles muy altos (como la pérdida de la vida cuando los datos de localización de personas protegidas caen en manos de delincuentes o cuando el suministro eléctrico se interrumpe de manera remota mediante dispositivos de medición inteligentes en condiciones meteorológicas o sanitarias críticas).

Estos dos elementos clave (la probabilidad de que el riesgo se materialice, por un lado, y la gravedad de las consecuencias, por otro) contribuyen cada uno de ellos a la evaluación global del impacto potencial.

Por último, al aplicar la metodología, deberá recordarse que la evaluación del impacto en virtud del artículo 7, letra f), no puede convertirse en un ejercicio mecánico y puramente cuantitativo. En los escenarios de evaluación de riesgos tradicionales, el concepto de «gravedad» puede tener en cuenta el número de individuos potencialmente afectados. Sin embargo, debería tenerse en consideración que el tratamiento de datos personales que tenga impacto sobre una minoría de interesados, o incluso sobre una sola persona, sigue exigiendo un análisis muy cuidadoso, especialmente si dicho impacto sobre cada persona afectada es potencialmente significativo.

ii) Naturaleza de los datos

En primer lugar, resulta importante evaluar si el tratamiento afecta a datos sensibles, bien porque pertenecen a las categorías especiales de datos en virtud del artículo 8 de la Directiva,

bien por otros motivos, como en el caso de los datos biométricos, la información genética, los datos de comunicación, los datos de localización y otro tipo de información personal que requiera una protección especial[86].

Sirva como ejemplo que, desde el punto de vista del Grupo de trabajo y como norma general, el uso de la biometría para cumplir requisitos de seguridad generales relativos a bienes o personas se considera un interés legítimo que no prevalecería sobre los intereses o derechos y libertades fundamentales del interesado. Por otro lado, los datos biométricos como las huellas digitales o el escaneo del iris podrían utilizarse para la seguridad de una zona de alto riesgo como un laboratorio que investigue virus peligrosos, siempre que el responsable del tratamiento haya presentado pruebas concretas de un riesgo considerable[87].

En general, cuanto más sensible sea la información en cuestión, más consecuencias podrá tener para el interesado. No obstante, esto no significa que los datos que parezcan en sí mismos y por sí mismos inocuos puedan tratarse libremente basándose en el artículo 7, letra f). Por supuesto, incluso dichos datos, dependiendo del modo en que se traten, podrán tener un impacto significativo sobre las personas, tal como se explicará en la subsección iii) posterior.

En este sentido, puede resultar pertinente el hecho de si los datos ya se han puesto a disposición del público por parte del interesado o por parte de terceros. En este caso, en primer lugar, es importante destacar que los datos personales, incluso si se han puesto a disposición del público, continúan considerándose datos personales, y su tratamiento, por tanto, continúa exigiendo las garantías adecuadas[88]. No existe una autorización general en virtud del artículo 7, letra f), para reutilizar y tratar posteriormente los datos personales puestos a disposición del público.

Dicho esto, el hecho de que los datos personales se pongan a disposición del público puede considerarse como un factor en la evaluación, especialmente si la publicación se llevó a cabo con una expectativa razonable de reutilización de los datos para determinados fines (por ejemplo, con fines de investigación o con fines relacionados con la transparencia y la responsabilidad).

iii) El modo en el que se tratan los datos

---

86 Los datos biométricos y la información genética se consideran categorías especiales de datos en la propuesta de Reglamento relativo a la protección de datos de la Comisión, junto con las enmiendas propuestas por la Comisión LIBE. Véase la enmienda 103 al artículo 9 del Informe final de la Comisión LIBE. Sobre la relación entre los artículos 7 y 8 de la Directiva 95/46/EC, véase la sección II.1.2 anterior en las páginas de 17 a 19.

87 Véase el Dictamen 3/2012 del Grupo de Trabajo del artículo 29 sobre la evolución de las tecnologías biométricas (WP193). Otro ejemplo: en su Dictamen 4/2009 sobre la Agencia Mundial Antidopaje (AMA) (citado anteriormente en el pie de página 32), el Grupo de trabajo puso de manifiesto que el artículo 7, letra f), no sería un fundamento jurídico válido para tratar datos médicos y datos relacionados con delitos en el contexto de investigaciones antidopaje, en vista de la «gravedad de las intrusiones en la intimidad». El tratamiento de datos deberá estar previsto por ley y cumplir los requisitos de los apartados 4) y 5) del artículo 8 de la Directiva.

88 Véase el Dictamen 3/2013 del Grupo de trabajo sobre la limitación de la finalidad (citado en el pie de página 9 anterior) y el Dictamen 06/2013 del Grupo de trabajo sobre datos abiertos y reutilización de la información del sector público (ISP), adoptado el 5 de junio de 2013 (WP207).

En la evaluación del impacto en un sentido más amplio se puede considerar el hecho de si los datos se han revelado al público o se han puesto de otra manera a disposición de un gran número de personas, o si una gran cantidad de datos personales se tratan o combinan con otros datos (por ejemplo, en el caso de la elaboración de perfiles, con fines mercantiles, con fines de cumplimiento de la ley u otros). Los datos aparentemente inocuos, cuando se tratan a gran escala y se combinan con otros datos, pueden dar lugar a injerencias en datos más sensibles, como se demuestra en el anterior escenario 3, que pone como ejemplo la relación entre los patrones de consumo de pizza y las primas de seguro de asistencia sanitaria.

Además de dar lugar, potencialmente, al tratamiento de datos más sensibles, dicho análisis puede llevar también a predicciones extrañas, inesperadas y a veces inexactas, por ejemplo, relativas al comportamiento o la personalidad de las personas afectadas. Dependiendo de la naturaleza y del impacto de dichas predicciones, esto puede resultar altamente intrusivo en la intimidad de la persona[89].

El Grupo de trabajo también destacó en un Dictamen previo los riesgos inherentes a determinadas soluciones de seguridad (incluidos los sistemas de filtrado del correo, eliminación de virus o protección contra las intrusiones) ya que pueden dar lugar a una implantación a gran escala de inspección profunda de paquetes, lo que puede tener una influencia significativa en la evaluación del equilibrio entre los derechos[90].

En general, cuanto más negativo e incierto pueda ser el impacto del tratamiento, más improbable es que el tratamiento se considere, en conjunto, legítimo. La disponibilidad de métodos alternativos para conseguir los objetivos perseguidos por el responsable del tratamiento, con menos impacto negativo sobre el interesado, debería ser, sin duda, una consideración pertinente en este contexto. Cuando proceda, las evaluaciones del impacto relativo a la protección de datos y a la intimidad pueden utilizarse para determinar si existe esta posibilidad.

iv) Expectativas razonables del interesado

Las expectativas razonables del interesado en relación con el uso y la revelación de datos también resultan muy pertinentes en este sentido. Tal como se puso de manifiesto con respecto al análisis del principio de limitación de la finalidad[91], es importante considerar si la posición del responsable de los datos[92], la naturaleza de la relación o del servicio prestado[93], o las obligaciones jurídicas o contractuales aplicables (u otras promesas hechas en el momento de la recopilación de los datos) podrían dar lugar a expectativas razonables de una confidencialidad más estricta y de limitaciones más estrictas relativas a su uso ulterior. En

89 Véase la sección III.2.5 y el anexo 2 (sobre macrodatos y datos abiertos) del Dictamen sobre la limitación de la finalidad (citado anteriormente en el pie de página 9).

90 Véase la sección 3.1 del Dictamen 1/2009 del Grupo de trabajo sobre las propuestas que modifican la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) (WP159).

91 Véanse las páginas 24 y 25 del Dictamen 3/2013 del Grupo de trabajo sobre la limitación de la finalidad (citado en el pie de página 9 anterior).

92 Como, por ejemplo, un abogado o un médico.

93 Como, por ejemplo, servicios de computación en nube para la gestión de documentación personal, servicios de correo electrónico, diarios, libros electrónicos equipados con funciones de toma de notas y diversas aplicaciones de registro de datos personales que puedan contener información muy personal.

general, cuanto más específico y restrictivo sea el contexto de la recopilación de los datos, más limitaciones es probable que se utilicen. En este caso, de nuevo, es necesario tener en cuenta el contexto fáctico y no basarse simplemente en la letra pequeña del texto.

v) Posición del responsable del tratamiento y del interesado

La posición del interesado y del responsable del tratamiento también es pertinente al evaluar el impacto del mismo. Dependiendo de si el responsable del tratamiento de los datos es una persona o una pequeña organización, una gran empresa multinacional o un organismo del sector público, y de las circunstancias específicas, su posición puede ser más o menos dominante respecto del interesado. Una empresa multinacional puede, por ejemplo, tener más recursos y poder de negociación que el interesado individual y, por tanto, puede encontrarse en una mejor posición para imponer al interesado lo que cree que corresponde a su «interés legítimo». Esto puede producirse con más razón si la empresa tiene una posición dominante en el mercado. Si estas situaciones no se corrigen, irán en perjuicio de los interesados individuales. Así como la legislación sobre competencia y protección de los consumidores ayuda a garantizar que no se utilice indebidamente este poder, la legislación sobre protección de datos también podría desempeñar un importante papel para asegurar que los derechos y los intereses de los afectados no se vean indebidamente perjudicados.

Por otro lado, la posición del interesado resulta también pertinente. Aunque la prueba de sopesamiento deberá hacerse en principio en relación con la persona con un perfil medio, las situaciones concretas deberán dar lugar a un enfoque más específico caso por caso: por ejemplo, sería pertinente considerar si el interesado es un niño[94] o pertenece de otro modo a algún segmento más vulnerable de la población que requiera protección especial, como, por ejemplo, los enfermos mentales, los solicitantes de asilo o las personas mayores. El hecho de si el interesado es un empleado, un estudiante, un paciente, o si existe de otro modo un desequilibrio en la relación entre la posición del interesado y la del responsable del tratamiento debe, sin duda, considerarse también relevante. Es importante evaluar el efecto del tratamiento real en las personas concretas.

Por último, es importante destacar que no todas las repercusiones negativas para los interesados «pesan» lo mismo en la balanza. La finalidad de la prueba de sopesamiento con arreglo al artículo 7, letra f), no es impedir cualquier impacto negativo sobre el interesado. Por el contrario, su finalidad es impedir un impacto desproporcionado. Esta es una diferencia crucial. Por ejemplo, la publicación de un artículo periodístico bien documentado y preciso sobre una supuesta corrupción gubernamental puede dañar la reputación de los cargos gubernamentales implicados y puede tener consecuencias significativas, incluida la pérdida de reputación, la pérdida de las elecciones, o la privación de libertad, pero podría seguir utilizando como fundamento el artículo 7, letra f)[95].

c) Equilibrio provisional

[94] Véase el Dictamen 2/2009 del Grupo de trabajo sobre la protección de los datos personales de los niños (Directrices generales y especial referencia a las escuelas) adoptado el 11 de febrero de 2009 (WP160). Este Dictamen insiste en la vulnerabilidad específica del niño y en caso de que el niño esté representado, en la necesidad de tener en cuenta el mejor interés del niño y no el de su representante.

[95] Tal como se explica anteriormente, también deberán tenerse en cuenta cualesquiera excepciones al tratamiento con fines periodísticos en virtud del artículo 9 de la Directiva.

A la hora de ponderar los intereses y los derechos en juego anteriormente descritos, las medidas adoptadas por el responsable del tratamiento para cumplir sus obligaciones generales en virtud de la Directiva, también en términos de proporcionalidad y transparencia, contribuirán en gran medida a garantizar que el responsable del tratamiento de los datos cumpla los requisitos del artículo 7, letra f). Pleno cumplimiento deberá significar que el impacto sobre las personas es reducido, que es *menos probable* que haya injerencia en los intereses o los derechos o libertades fundamentales de los interesados y que, por tanto, es *más probable* que el responsable del tratamiento de los datos pueda utilizar como fundamento jurídico el artículo 7, letra f). Esto deberá alentar a los responsables del tratamiento a cumplir mejor todas las disposiciones horizontales de la Directiva[96].

No obstante, esto no significa que el cumplimiento de estos requisitos horizontales por sí mismo sea siempre suficiente para garantizar una base jurídica basada en el artículo 7, letra f). De hecho, si este fuera el caso, el artículo 7, letra f), sería superfluo o daría lugar a una laguna que privaría de sentido al artículo 7 en su conjunto, ya que este insta a tener una base jurídica específica adecuada para el tratamiento.

Por este motivo, es importante llevar a cabo una evaluación adicional en la prueba de sopesamiento en los casos en que, basándose en análisis preliminares, no quede claro cómo alcanzar un equilibrio. El responsable del tratamiento de los datos puede considerar si es posible adoptar medidas adicionales, yendo más allá del cumplimiento de las disposiciones horizontales de la Directiva, para ayudar a reducir el impacto indebido del tratamiento sobre los interesados.

Las medidas adicionales podrán comprender, por ejemplo, la facilitación de un mecanismo viable y accesible para garantizar la posibilidad incondicional de que los interesados se excluyan voluntariamente del tratamiento. Estas medidas adicionales podrán, en algunos casos (aunque no en todos), ayudar a inclinar la balanza y a garantizar que el tratamiento pueda basarse en el artículo 7, letra f), mientras que se protejan al mismo tiempo los derechos y los intereses de los interesados.

d) Garantías adicionales aplicadas por el responsable del tratamiento

Tal como se explica anteriormente, el modo en el que el responsable del tratamiento adopte las medidas adecuadas podría, en algunas situaciones, ayudar a «inclinar la balanza». El hecho de que el resultado sea o no aceptable dependerá de la evaluación en su conjunto. Cuanto más significativo sea el impacto sobre el interesado, más atención deberá prestarse a las garantías pertinentes.

Ejemplos de medidas pertinentes podrán comprender, entre otros, una limitación estricta de la cantidad de datos recopilados, o su eliminación inmediata tras su uso. Aunque algunas de estas medidas pueden ser ya obligatorias en virtud de la Directiva, son con frecuencia modulables y dejan margen para que los responsables del tratamiento garanticen una mejor protección de los interesados. Por ejemplo, el responsable del tratamiento puede recopilar menos datos o facilitar información adicional en relación con lo enumerado de manera específica en los artículos 10 y 11 de la Directiva.

[96] Sobre el importante papel del cumplimiento horizontal, véase también la página 54 del Dictamen 3/2013 del Grupo de trabajo sobre la limitación de la finalidad, citado en el pie de página 9 anterior.

En algunos casos, estas garantías no se exigen *de manera explícita* en virtud de la Directiva, aunque podrían exigirse en el futuro de conformidad con la propuesta de Reglamento, o solo se exigen en situaciones específicas. Algunos ejemplos de estas garantías son:

- medidas técnicas y organizativas para garantizar que los datos no puedan utilizarse con el fin de adoptar medidas o emprender otras acciones en relación con las personas («separación funcional» como es, con frecuencia, el caso en el contexto científico);
- uso extensivo de técnicas de anonimización;
- agregación de datos;
- tecnologías de protección de la intimidad, protección de la privacidad desde el diseño, evaluaciones del impacto relativo a la protección de datos y a la intimidad;
- aumento de la transparencia;
- derecho general e incondicional de exclusión voluntaria;
- portabilidad de los datos y medidas relacionadas para capacitar a los interesados.

El Grupo de trabajo pone de manifiesto que, en relación con algunas cuestiones clave, incluidas la separación funcional y las técnicas de anonimización, ya se han facilitado algunas directrices en las partes pertinentes de sus Dictámenes sobre la limitación de la finalidad, sobre datos abiertos y sobre las técnicas de anonimización[97].

En lo referente a la seudonimización y el cifrado, el Grupo de trabajo desea enfatizar que el hecho de que los datos no sean directamente identificables no afecta como tal a la apreciación de la legitimidad del tratamiento: no deberá entenderse como la conversión de un proceso ilegítimo en uno legítimo[98].

Al mismo tiempo, la seudonimización y el cifrado, como cualesquiera otras medidas técnicas y organizativas adoptadas para proteger la información personal, desempeñarán un papel respecto de la evaluación del impacto potencial del tratamiento sobre el interesado y, por tanto, podrán a veces hacer inclinarse la balanza a favor del responsable del tratamiento. La utilización de formas menos arriesgadas de tratamiento de datos personales (por ejemplo, datos personales cifrados mientras estén almacenados o en tránsito, o datos personales que sean menos directa y fácilmente identificables) deberá generalmente significar que la probabilidad de que se produzca una injerencia en los intereses o los derechos y libertades fundamentales de los interesados es reducida.

En relación con estas garantías, y con la evaluación global del equilibrio, el Grupo de trabajo desea destacar tres cuestiones específicas que con frecuencia desempeñan un papel crucial en el contexto del artículo 7, letra f):

---

97 Véanse las secciones III.2.3, III.2.5 y el anexo 2 del Dictamen 3/2013 del Grupo de trabajo sobre la limitación de la finalidad, citado anteriormente en el pie de página 9, sobre el tratamiento ulterior de datos con fines históricos, estadísticos o científicos, y sobre macrodatos y datos abiertos; véanse también las partes pertinentes del Dictamen 06/2013 del Grupo de trabajo sobre datos abiertos (citado en el pie de página 88 anterior) y del Dictamen 5/2014 sobre técnicas de anonimización.

98 Véanse, a este respecto, las enmiendas votadas por la Comisión LIBE en su Informe final y en especial la enmienda 15 al considerando 38 relacionando la seudonimización y las expectativas legítimas del interesado.

- la relación entre la prueba de sopesamiento, la transparencia y el principio de responsabilidad;
- el derecho de oposición al tratamiento por parte del interesado, y más allá de la oposición, la posibilidad de exclusión voluntaria sin la necesidad de justificación; y
- la capacitación de los interesados: la portabilidad de los datos y la existencia de mecanismos viables para que el interesado acceda, modifique, elimine, transfiera o de otro modo reutilice (o permita reutilizar a terceros) sus propios datos.

Debido a su importancia, estas cuestiones se debatirán en rúbricas separadas.

III.3.5. Responsabilidad y transparencia

En primer lugar, antes de que tenga lugar una operación de tratamiento basada en el artículo 7, letra f), el responsable del tratamiento tiene la responsabilidad de evaluar si tiene un interés legítimo, si el tratamiento es necesario para dicho interés legítimo y si dicho interés prevalece sobre los intereses y los derechos de los afectados en ese caso específico.

En este sentido, el artículo 7, letra f), se basa en el principio de responsabilidad. El responsable del tratamiento debe llevar a cabo un examen cuidadoso y eficaz de antemano, basado en los hechos específicos del caso y no de manera abstracta, teniendo en cuenta las expectativas razonables de los interesados. Como cuestión de buena práctica, cuando así proceda, la realización de este examen deberá documentarse de manera suficientemente detallada y transparente, para que la aplicación correcta y completa del examen pueda ser verificada, cuando sea necesario, por las partes interesadas pertinentes, incluidos los interesados y las autoridades de protección de datos y, en última instancia, por los tribunales.

El responsable del tratamiento definirá, en primer lugar, el interés legítimo y efectuará la prueba de sopesamiento, pero esta no será necesariamente la evaluación final y definitiva: si el interés considerado no es, en realidad, el especificado por el responsable del tratamiento o si este no definió el interés con suficiente detalle, el equilibrio deberá volver a ponderarse, basándose en el interés real, que será determinado bien por la autoridad de protección de datos bien por un tribunal[99]. Al igual que en otros aspectos clave de la protección de datos, como la identificación del responsable del tratamiento de datos o la especificación de la finalidad[100], lo que importa es la realidad que haya detrás de cada afirmación hecha por el responsable del tratamiento.

El concepto de responsabilidad está íntimamente ligado al concepto de transparencia. Con el fin de permitir que los interesados ejerciten sus derechos y que haya un escrutinio público más amplio por parte de los interesados, el Grupo de trabajo recomienda que los responsables del tratamiento expliquen a los interesados de manera clara y fácil las razones por las que creen que sus intereses prevalecen sobre los intereses o los derechos y las libertades fundamentales de los interesados, y también les expliquen las garantías que hayan adoptado para proteger sus datos personales, incluido, cuando así proceda, el derecho de exclusión voluntaria del tratamiento[101].

---

99 Por ejemplo, tras una queja o una oposición conforme al artículo 14.

100 Véanse los Dictámenes citados en el pie de página 9.

101 Tal como se explica en la página 46 del Dictamen 3/2013 del Grupo de trabajo sobre la limitación de la finalidad (citado en el pie de página 9 anterior), en el caso de la elaboración de perfiles y la toma de decisiones automatizada, se deberá dar acceso a los interesados o consumidores a sus perfiles para

En este sentido, el Grupo de trabajo enfatiza que la legislación de protección de los consumidores, en especial, las leyes que protegen a los consumidores contra las prácticas comerciales injustas, resultan aquí especialmente pertinentes.

El hecho de que el responsable del tratamiento oculte información importante relativa a una reutilización inesperada de los datos escondida en términos legalistas en la letra pequeña de un contrato puede infringir la normativa de protección de los consumidores en materia de cláusulas contractuales abusivas (incluida la prohibición de las cláusulas «sorpresa»), y tampoco cumplirá los requisitos del artículo 7, letra a), de un consentimiento válido e informado o los requisitos de la letra f) del mismo artículo en términos de expectativas razonables del interesado y de un equilibrio de intereses global aceptable. También plantearía, por supuesto, cuestiones relativas al cumplimiento del artículo 6 respecto de la necesidad de un tratamiento leal y lícito de los datos personales.

Por ejemplo, en una serie de casos, los usuarios de servicios en línea «gratuitos», como búsquedas, correo electrónico, medios sociales, almacenamiento de archivos u otras aplicaciones móviles o en línea, no son completamente conscientes de en qué medida su actividad se registra y analiza con el fin de generar valor para el proveedor de servicios y, por tanto, no son conscientes de los riesgos asumidos.

Con el fin de capacitar a los interesados en estas situaciones, una condición previa[102] necesaria, aunque en ningún caso suficiente en sí misma, es dejar claro que los servicios no son gratuitos sino que los consumidores pagan permitiendo la utilización de sus datos personales. Las condiciones y las garantías según las cuales puedan utilizarse los datos deberán quedar claramente definidas en cada caso para garantizar la validez del consentimiento del artículo 7, letra a), o un equilibrio favorable en virtud del artículo 7, letra f).

III.3.6. El derecho de oposición y más allá

a) El derecho de oposición en virtud del artículo 14 de la Directiva

Las letras e) y f) del artículo 7 son especiales en el sentido de que, si bien se basan principalmente en una evaluación objetiva de los intereses y de los derechos en cuestión, también permiten la libertad de decisión del interesado gracias al derecho de oposición[103]: al

---

garantizar la transparencia, así como a la lógica del proceso de toma de decisiones (algoritmo) que dio lugar al desarrollo de dichos perfiles. En otras palabras: las organizaciones deberán revelar sus criterios para la toma de decisiones. Se trata de una garantía fundamental y resulta especialmente importante en el mundo de los macrodatos. El hecho de que una organización ofrezca o no esta transparencia es un factor muy pertinente que se deberá considerar también en la prueba de sopesamiento.

102 Para posibles garantías adicionales en relación con las situaciones cada vez más comunes en las que los consumidores pagan con sus datos personales, véase la sección III.3.6, en especial las páginas 55 y 56 sobre «Alternativas, con garantías para la protección de datos, a los servicios "gratuitos" en línea» y sobre «Portabilidad de los datos, "midata" y cuestiones relacionadas».

103 El derecho de oposición no deberá confundirse con el caso del consentimiento basado en el artículo 7, letra a), en el que el responsable del tratamiento de los datos no puede tratarlos antes de obtener dicho consentimiento. En el contexto del artículo 7, letra f), el responsable del tratamiento puede tratar los datos, sujeto a determinadas condiciones y garantías, siempre que el interesado no se haya opuesto. En este sentido, el derecho de oposición puede considerarse más bien una forma específica de exclusión voluntaria.

menos en el caso de estos dos motivos de legitimación, el artículo 14, letra a), de la Directiva estipula que («salvo cuando la legislación nacional disponga otra cosa») el interesado «puede oponerse […] en cualquier momento y por razones legítimas propias de su situación particular, a que los datos que le conciernan sean objeto de tratamiento». Añade que si la oposición es justificada, el tratamiento de los datos debe cesar.

En principio, de conformidad con la legislación actual, el interesado deberá, pues, demostrar «interés legítimo» para interrumpir el tratamiento de sus datos personales (artículo 14, letra a)), excepto en el contexto de las actividades de prospección, en las que la oposición no necesita justificarse (artículo 14, letra b)).

Esto no deberá entenderse en contradicción con la prueba de sopesamiento del artículo 7, letra f), que se efectúa *a priori*: más bien complementa el equilibrio, en el sentido de que, cuando se permite el tratamiento tras una evaluación razonable y objetiva de los diferentes derechos e intereses en juego, el interesado todavía tiene la posibilidad *adicional* de oposición basándose en motivos de legitimación relativos a su situación particular. Esto deberá dar lugar a una nueva evaluación que tenga en cuenta los argumentos concretos presentados por el interesado. Esta nueva evaluación quedará, en principio, sujeta de nuevo a verificación por las autoridades de protección de datos o por los tribunales.

b) Más allá de la oposición: la exclusión voluntaria como garantía adicional

El Grupo de trabajo destaca que, incluso si el derecho de oposición del artículo 14, letra a), está sujeto a justificación por parte del interesado, nada impide que el responsable del tratamiento ofrezca una cláusula de exclusión voluntaria más amplia, que no requiera ninguna demostración adicional de interés legítimo (apremiante o de otro modo) por parte del interesado. Dicho derecho incondicional no necesitaría basarse en la situación específica de los interesados.

De hecho, y especialmente en casos dudosos en los que sea difícil encontrar un equilibrio, un mecanismo de exclusión voluntaria viable y bien diseñado, aunque no ofrezca necesariamente a los interesados todas las garantías de un consentimiento válido en virtud del artículo 7, letra a), podría desempeñar un papel fundamental para salvaguardar los derechos y los intereses de los afectados.

Con este fin se requiere un enfoque matizado que distinga entre los casos en los que se exige un consentimiento de inclusión voluntaria conforme al artículo 7, letra a), y los casos en los que una posibilidad viable de exclusión voluntaria del tratamiento (combinada con otras posibles medidas adicionales) pueda contribuir a la protección de los interesados en virtud del artículo 7, letra f).

Cuanto más ampliamente aplicable sea el mecanismo de exclusión voluntaria y más fácil sea ejercerlo, más contribuirá a inclinar la balanza en favor del tratamiento el hecho de encontrar un fundamento jurídico basado en el artículo 7, letra f).

Ejemplo: la evolución en el enfoque de la prospección

Véanse más detalles en el Dictamen 15/2011 del Grupo de trabajo sobre la definición del consentimiento (citado en el pie de página 2).

Para ilustrar la distinción entre los casos en que se exige un consentimiento conforme al artículo 7, letra a), y los casos en los que se podría utilizar una cláusula de exclusión voluntaria como garantía en virtud del artículo 7, letra f), resulta útil el ejemplo de la prospección, en relación con la cual ha existido tradicionalmente una disposición de exclusión voluntaria específica incluida en el artículo 14, letra b), de la Directiva. Con el fin de hacer frente a los nuevos avances tecnológicos, esta disposición se ha complementado después mediante disposiciones específicas en la Directiva sobre intimidad y comunicaciones electrónicas[104].

En virtud del artículo 13 de la Directiva sobre intimidad y comunicaciones electrónicas, para determinados tipos, más intrusivos, de actividades de prospección (como la comercialización mediante correo electrónico y los sistemas de llamada automática) el consentimiento es la norma. Como excepción, en relaciones ya existentes con clientes en las que el responsable del tratamiento publicita sus propios productos o servicios «similares», es suficiente ofrecer una posibilidad (incondicional) de «exclusión voluntaria» sin justificación.

La evolución de la tecnología ha exigido soluciones similares, relativamente sencillas y que siguen una lógica parecida, para las nuevas prácticas de mercadotecnia.

En primer lugar, ha evolucionado la manera en la que se entrega el material de comercialización: en vez de sencillos correos electrónicos que llegan a los buzones de correo, en la actualidad aparece en las pantallas de los teléfonos inteligentes y de los ordenadores publicidad dirigida basada en el comportamiento. En un futuro próximo, la publicidad podrá también estar incluida en dispositivos inteligentes conectados a la Internet de los objetos.

En segundo lugar, la publicidad está orientada de manera cada vez más específica: en vez de basarse en perfiles sencillos de cliente, con más frecuencia se hace un seguimiento de las actividades de los consumidores y los datos se almacenan en línea y fuera de línea, y se analizan con métodos automatizados más sofisticados[105].

Como resultado de esta evolución, el objeto de la prueba de sopesamiento ha variado: la cuestión no es ya el derecho de libertad de expresión comercial, sino principalmente el interés económico de las organizaciones empresariales en conocer a sus clientes haciendo un seguimiento y supervisando sus actividades en línea y fuera de línea, que deberá ponderarse en relación con los derechos (fundamentales) a la intimidad y a la protección de los datos personales de estas personas y su interés en no ser indebidamente supervisadas.

Este cambio en los modelos comerciales dominantes y el aumento del valor de los datos personales como activo para las organizaciones empresariales explica el reciente requisito de consentimiento en este contexto, de conformidad con el artículo 5, apartado 3, y con el artículo 13 de la Directiva sobre intimidad y comunicaciones electrónicas.

---

104 Sobre el artículo 13 de la Directiva sobre intimidad y comunicaciones electrónicas, véase también la sección III.2.4 del Dictamen 3/2013 del Grupo de trabajo sobre la limitación de la finalidad (citado en el pie de página 9 anterior).

105 Véase la sección III.2.5 y el anexo 2 (sobre macrodatos y datos abiertos) del Dictamen 3/2013 del Grupo de trabajo sobre la limitación de la finalidad (citado anteriormente en el pie de página 9).

Existen, por tanto, diferentes normas específicas que dependen de la forma de comercialización, a saber:

- el derecho incondicional de oposición a la prospección (concebido en el contexto del correo postal tradicional para la comercialización de productos similares) en virtud del artículo 14, letra b), de la Directiva; el artículo 7, letra f), podría ser el fundamento jurídico en ese caso;
- el requisito del consentimiento en virtud del artículo 13 de la Directiva sobre intimidad y comunicaciones electrónicas para sistemas de llamada automática, comercialización mediante correo electrónico, fax y mensajes de texto (sujeto a excepciones)[106], y la aplicación *de facto* del artículo 7, letra a), de la Directiva de protección de datos.
- el requisito del consentimiento en virtud del artículo 5, apartado 3, de la Directiva sobre intimidad y comunicaciones electrónicas (y el artículo 7, letra a), de la Directiva de protección de datos) en el caso de publicidad comportamental basada en técnicas de seguimiento tales como cookies que almacenan información en el terminal del usuario[107].

Mientras que los motivos de legitimación aplicables son claros en lo que se refiere al artículo 5, apartado 3, y al artículo 13 de la Directiva sobre intimidad y comunicaciones electrónicas, estos no cubren todas las formas de comercialización y sería deseable contar con directrices sobre las situaciones en las que se requiera el consentimiento del artículo 7, letra a), y para las que sea necesario encontrar un equilibrio en virtud del artículo 7, letra f), incluyendo una posibilidad de exclusión voluntaria.

En este sentido, resulta útil recordar el Dictamen del Grupo de trabajo sobre la limitación de la finalidad, donde se afirmaba concretamente que cuando una organización desea analizar o predecir de manera específica las preferencias personales, el comportamiento y las actitudes de los clientes individuales que posteriormente motivarán las «decisiones o medidas» adoptadas en relación con dichos clientes... debería exigirse casi siempre un consentimiento gratuito, específico, informado e inequívoco de «inclusión voluntaria», pues de otro modo la reutilización de los datos no podrá considerarse compatible. Y lo que es más importante, dicho consentimiento deberá exigirse, por ejemplo, para el seguimiento y la elaboración de perfiles con fines de prospección , publicidad comportamental, comercialización de datos, publicidad basada en la localización, o investigación digital de mercado basada en el seguimiento[108].

Alternativas, con garantías para la protección de datos, a los servicios «gratuitos» en línea

En el contexto en el que los clientes que contratan servicios en línea «gratuitos» «pagan» de hecho estos servicios permitiendo la utilización de sus datos personales, si el responsable del tratamiento también ofrece una versión alternativa de sus servicios, en la que los «datos personales» no sean utilizados con fines de comercialización, también contribuirá a una

[106] Véase también el artículo 13, apartado 3, de la Directiva sobre intimidad y comunicaciones electrónicas, que permite a los Estados miembros la elección entre el consentimiento o una cláusula de inclusión y exclusión voluntaria en el caso de prospección mediante otros medios.

[107] Véase, para la aplicación de esta disposición, el Dictamen 2/2010 del Grupo de trabajo sobre publicidad comportamental en línea (WP171).

[108] Véase el anexo II (sobre macrodatos y datos abiertos) del Dictamen (citado en el pie de página 9 anterior), página 45.

evaluación favorable del equilibrio, o a la conclusión de que el cliente tiene auténtica libertad de elección y, por tanto, se cumple el consentimiento válido en virtud del artículo 7), letra a).

En la medida en que dichos servicios alternativos no estén disponibles, será más difícil argumentar que se ha concedido un consentimiento válido (otorgado libremente) en virtud del artículo 7, letra a), por el mero uso de servicios gratuitos, o argumentar que, en virtud del artículo 7, letra f), la balanza se inclina a favor del responsable del tratamiento.

Las consideraciones anteriores subrayan el importante papel que las garantías adicionales, incluido un mecanismo viable de exclusión voluntaria del tratamiento, pueden desempeñar para modificar el equilibrio provisional. Al mismo tiempo, también sugieren que en algunos casos el artículo 7, letra f), no puede utilizarse como fundamento jurídico del tratamiento y los responsables del mismo deben garantizar un consentimiento válido en virtud del artículo 7, letra a), o cumplir otras condiciones de la Directiva, para que se lleve a cabo el tratamiento.

Portabilidad de los datos, «midata» y cuestiones relacionadas

Entre las garantías adicionales que pueden ayudar a inclinar la balanza, deberá prestarse especial atención a la portabilidad de los datos y a las medidas relacionadas, que pueden ser cada vez más pertinentes en un entorno en línea. El Grupo de trabajo se remite a su Dictamen sobre la limitación de la finalidad, en el que destacó que, en muchas situaciones, las garantías tales como permitir que los interesados o los clientes tengan acceso directo a sus datos en un formato portable, fácil de usar y legible por máquina puede ayudar a darles poder y a reducir el desequilibrio económico entre las grandes empresas, por un lado, y los interesados o consumidores, por otro. También permitiría que las personas «compartieran la riqueza» creada por los macrodatos e incentivaría a los promotores a ofrecer funciones y aplicaciones adicionales a sus usuarios[109].

La disponibilidad de mecanismos viables para que los interesados accedan, modifiquen, eliminen, transfieran o de otro modo reutilicen (o permitan a terceros reutilizar) sus propios datos otorgará poder a los interesados y les permitirá beneficiarse en mayor medida de los servicios digitales. Además, esto puede fomentar un entorno de mercado más competitivo, permitiendo a los clientes cambiar de proveedores más fácilmente (por ejemplo, en el contexto de la banca en línea o en el caso de proveedores de energía en un entorno de redes inteligentes). Por último, puede también contribuir al desarrollo de servicios adicionales de valor añadido por parte de terceros que puedan acceder a los datos de los clientes a petición de éstos y basándose en su consentimiento. Desde esta perspectiva, la portabilidad de los datos, por tanto, no es solo buena para la protección de los datos sino también para la competencia y la protección de los consumidores[110].

---

109 Véanse iniciativas como «midata» en el Reino Unido, que se basa en el principio clave de que los datos deberán devolverse a los consumidores. Midata es un programa voluntario, que proporcionará con el tiempo a los consumidores un mayor acceso a sus datos personales en un formato electrónico portable. La idea central es que los consumidores deben beneficiarse también de los macrodatos teniendo acceso a su propia información de manera que puedan elegir mejor. Véanse también las iniciativas «Botón verde», que permiten el acceso de los consumidores a la información sobre su uso de la energía. Para más información sobre iniciativas en el Reino Unido y Francia véase http://www.midatalab.org.uk/ y http://mesinfos.fing.org/.

110 Sobre el derecho a la portabilidad de los datos, véase el artículo 18 de la propuesta de Reglamento.

IV. Observaciones finales

En el presente Dictamen, el Grupo de trabajo ha analizado los principios establecidos en el artículo 7 de la Directiva relativos a la legitimación del tratamiento de datos. Más allá de la orientación sobre la interpretación y la aplicación prácticas del artículo 7, letra f), de conformidad con el marco jurídico vigente, tiene el objetivo de formular recomendaciones políticas para facilitar a los responsables políticos la toma de decisiones a la hora de modificar el marco jurídico vigente sobre la protección de datos. Antes de formular dichas recomendaciones, se resumen a continuación las principales conclusiones relativas a la interpretación del artículo 7.

IV.1. Conclusiones

Sinopsis del artículo 7

En el artículo 7 se exige que sea aplicable al menos uno de los seis fundamentos jurídicos de dicho artículo para permitir el tratamiento de datos personales.

Su primer fundamento jurídico, contenido en el artículo 7, letra a), se centra en el consentimiento del interesado como motivo de legitimidad. Los demás motivos, por el contrario, permiten el tratamiento, sujeto a garantías, en situaciones en las que, independientemente del consentimiento, resulte apropiado y necesario tratar los datos en un determinado contexto en la búsqueda de un interés legítimo específico.

En cada una de las letras b), c), d) y e) se especifica un contexto concreto, en el que el tratamiento de los datos personales puede considerarse legítimo. Las condiciones aplicables a cada uno de estos diferentes contextos requieren atención cuidadosa, ya que determinan el ámbito de los diferentes motivos de legitimidad. De manera más específica, los criterios «necesarios para la ejecución de un contrato», «necesarios para el cumplimiento de una obligación jurídica», «necesarios para proteger el interés vital del interesado» y «necesarios para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público» contienen diferentes requisitos que se han debatido en la sección III.2.

La letra f) se refiere, de manera más general, a (cualquier clase de) interés legítimo perseguido por el responsable del tratamiento (en cualquier contexto). Esta disposición general, sin embargo, se supedita de manera específica a una prueba adicional de sopesamiento que pondere el interés legítimo del responsable del tratamiento o del tercero o terceros a los que se comuniquen los datos, en relación con los intereses o los derechos fundamentales de los interesados.

Función del artículo 7, letra f)

El artículo 7, letra f), no deberá considerarse un fundamento jurídico que solo puede utilizarse con moderación para cubrir las lagunas en situaciones raras o imprevistas como «un último recurso», o como una última posibilidad si no se pueden aplicar otros motivos de legitimación. Tampoco deberá percibirse como una opción preferente ni deberá extenderse su uso indebidamente porque se considere menos restrictiva que los demás fundamentos

jurídicos. Por el contrario, se trata de un medio tan válido como cualquier otro para legitimar el tratamiento de datos personales.

Una utilización apropiada del artículo 7, letra f), en las circunstancias correctas y sujeta a las garantías pertinentes, puede ayudar a impedir un uso indebido y a evitar una dependencia excesiva de otros fundamentos jurídicos. Una evaluación adecuada del equilibrio en virtud del artículo 7, letra f), en ocasiones con una posibilidad de exclusión voluntaria del tratamiento, puede en algunos casos ser una alternativa válida al uso inapropiado, por ejemplo, del fundamento jurídico basado en el «consentimiento» o en la «necesidad de ejecución de un contrato». Considerado de este modo, el artículo 7, letra f), presenta garantías complementarias en comparación con otros motivos de legitimación determinados previamente. No deberá, por tanto, considerarse como «el vínculo más débil» o una puerta abierta para legitimar todas las actividades de tratamiento de datos que no estén comprendidas en cualquiera de los demás motivos de legitimación.

Interés legítimo del responsable del tratamiento/intereses o derechos fundamentales del interesado

El concepto de «interés» es la implicación más amplia que el responsable del tratamiento pueda tener en el tratamiento, o el beneficio que este obtenga, o que la sociedad pueda obtener, del tratamiento. Este puede ser apremiante, claro o controvertido. Las situaciones a las que hace referencia el artículo 7, letra f), pueden variar, por tanto, del ejercicio de derechos fundamentales o la protección de intereses personales o sociales importantes a otros contextos menos obvios o incluso problemáticos.

Para que se considere «legítimo» y sea pertinente en virtud del artículo 7, letra f), el interés deberá ser lícito, es decir, conforme a la legislación nacional y de la UE. Debe estar articulado también con la claridad suficiente y debe ser lo suficientemente específico para permitir que la prueba de sopesamiento se realice en contraposición a los intereses y los derechos fundamentales del interesado. Debe también representar un interés real y actual, es decir, no debe ser especulativo.

Si el responsable del tratamiento o el tercero al que se comuniquen los datos tiene dicho interés legítimo, esto no significa necesariamente que se pueda utilizar el artículo 7, letra f), como fundamento jurídico del tratamiento. El hecho de que el artículo 7, letra f), pueda utilizarse como fundamento jurídico o no dependerá del resultado de la prueba de sopesamiento siguiente. El tratamiento debe ser también «necesario para la satisfacción del interés legítimo» perseguido por el responsable del tratamiento o, en el caso de revelación de los datos, por la tercera parte. Por tanto, siempre se preferirán medios menos invasivos para servir al mismo fin.

El concepto de «intereses» de los afectados se define incluso de manera más amplia, puesto que no requiere el elemento de «legitimidad». Si el responsable del tratamiento o la tercera parte pueden perseguir cualquier interés, siempre que no sea ilegítimo, el interesado a su vez tendrá derecho a que se tengan en cuenta todas las categorías de intereses que le afecten y a que se ponderen en relación con los intereses del responsable del tratamiento o la tercera parte, en tanto en cuanto estén comprendidos en el ámbito de la Directiva.

Aplicación de la prueba de sopesamiento

Al interpretar el ámbito del artículo 7, letra f), el Grupo de trabajo aspira a un enfoque equilibrado que garantice la flexibilidad necesaria a los responsables del tratamiento de datos en situaciones en las que no exista un impacto indebido sobre los interesados, mientras que, al mismo tiempo, se les proporcione una seguridad jurídica y unas garantías suficientes para que esta disposición abierta no se utilice indebidamente.

Para llevar a cabo esta prueba de sopesamiento, es importante considerar, en primer lugar, la naturaleza y la fuente del interés legítimo, y si el tratamiento es necesario para perseguir dicho interés, por un lado, y las repercusiones para los interesados, por otro. Esta evaluación inicial deberá tener en cuenta las medidas, como la transparencia o la recopilación limitada de datos, que el responsable del tratamiento se propone adoptar para cumplir con la Directiva.

Tras analizar y sopesar los dos lados de la balanza, puede establecerse un «equilibrio» provisional: puede extraerse una conclusión preliminar sobre si el interés legítimo del responsable del tratamiento prevalece sobre los derechos y los intereses de los afectados. Habrá casos, sin embargo, en los que el resultado de la prueba de sopesamiento no esté claro, y se alberguen dudas acerca de si el interés legítimo del responsable del tratamiento (o la tercera parte) prevalece y si el tratamiento puede basarse en el artículo 7, letra f).

Por este motivo, es importante llevar a cabo una valoración adicional en el ejercicio de sopesamiento. En esta fase, el responsable del tratamiento puede considerar si es posible introducir medidas adicionales, que vayan más allá del cumplimiento de las disposiciones horizontales de la Directiva, con el fin de facilitar la protección de los interesados. Las medidas adicionales podrán comprender, por ejemplo, la puesta a disposición de un mecanismo viable y accesible para garantizar la posibilidad incondicional de que los interesados se excluyan voluntariamente del tratamiento.

Factores clave que deben considerarse al efectuar la prueba de sopesamiento

Sobre la base de lo expuesto anteriormente, algunos factores útiles que deben considerarse cuando se lleve a cabo una prueba de sopesamiento son los siguientes:

- la naturaleza y fuente del interés legítimo, incluido el hecho de:

  - si el tratamiento de datos es necesario para el ejercicio de un derecho fundamental, o
  - si se trata, de otro modo, de una cuestión de interés público o que se beneficia del reconocimiento jurídico o normativo, social o cultural de la comunidad afectada.

- el impacto sobre los interesados, incluidas:

  - la naturaleza de los datos, por ejemplo, si el tratamiento afecta a datos que puedan considerarse sensibles o que consten en fuentes accesibles al público;
  - la manera en la que se tratan los datos, por ejemplo, si los datos se han revelado al público o se han puesto de otra manera a disposición de un gran número de personas, o si grandes cantidades de datos personales se tratan o combinan con otros datos (por ejemplo, en el caso de la elaboración de perfiles, con fines comerciales, de cumplimiento de la ley u otros);

- las expectativas razonables del interesado, especialmente en relación con el uso y la revelación de los datos en el contexto pertinente;
- la posición del responsable del tratamiento y del interesado, incluido el equilibrio de poder entre ambos, o si el interesado es un niño o pertenece de otro modo a un segmento vulnerable de la población.

- las garantías adicionales para impedir un impacto indebido sobre los interesados, incluidas:

- la minimización de los datos (por ejemplo, limitaciones estrictas sobre la recopilación de datos o su eliminación inmediata tras su uso);
- medidas técnicas y organizativas para garantizar que los datos no puedan utilizarse con el fin de adoptar medidas o emprender otras acciones en relación con las personas («separación funcional»);
- uso extensivo de técnicas de anonimización, agregación de datos, tecnologías de protección de la intimidad, protección de la privacidad desde el diseño, evaluaciones del impacto relativo a la protección de datos y a la intimidad;
- aumento de la transparencia, derecho general e incondicional de exclusión voluntaria, portabilidad de los datos y medidas relacionadas para capacitar a los interesados.

Responsabilidad, transparencia, derecho de oposición y más allá

En relación con estas garantías, y con la evaluación global del equilibrio, tres cuestiones desempeñan con frecuencia un papel crucial en el contexto del artículo 7, letra f), y, por tanto, requieren especial atención:

- la existencia o la posible necesidad de medidas adicionales para aumentar la transparencia y la responsabilidad;
- el derecho de oposición al tratamiento por parte del interesado, y más allá de la oposición, la posibilidad de exclusión voluntaria sin la necesidad de justificación; y
- el empoderamiento de los interesados: la portabilidad de los datos y la disponibilidad de mecanismos viables para que el interesado acceda, modifique, elimine, transfiera o de otro modo reutilice (o permita reutilizar a terceros) sus propios datos.

IV. 2. Recomendaciones

El texto actual del artículo 7, letra f), de la Directiva queda abierto. Esta redacción flexible deja mucho margen a la interpretación y, tal como demuestra la experiencia, ha dado lugar a veces a una falta de previsibilidad y de seguridad jurídicas. No obstante, si se utiliza en el contexto adecuado, y con la aplicación de los criterios adecuados, tal como se establecen en este Dictamen, el artículo 7, letra f), tiene un papel esencial que desempeñar como fundamento jurídico del tratamiento de datos.

El Grupo de trabajo, por tanto, apoya el enfoque actual del artículo 6 de la propuesta de Reglamento, que mantiene el equilibrio de intereses como un fundamento jurídico separado. No obstante, sería deseable contar con orientaciones adicionales para garantizar una aplicación adecuada de la prueba de sopesamiento.

Ámbito y medios de especificación adicional

Un requisito esencial sería que la disposición siga siendo lo suficientemente flexible y que refleje tanto la perspectiva del responsable del tratamiento de datos como la del interesado, así como la naturaleza dinámica de los contextos pertinentes. Por este motivo, el Grupo de trabajo considera que no es aconsejable facilitar, en el texto de la propuesta de Reglamento o en los actos delegados, listas detalladas y exhaustivas de situaciones en las que un interés sea calificado *de facto* como legítimo. El Grupo de trabajo también se opone a la definición de casos en los que el interés o el derecho de una parte deba *por principio* o *por presunción* prevalecer sobre el interés o el derecho de la otra parte, exclusivamente debido a la naturaleza de dicho interés o derecho, o porque se hayan adoptado determinadas medidas protectoras, por ejemplo, el mero hecho de que los datos se hayan seudoanonimizado. En este caso se correría el riesgo de que resulte ambiguo o innecesariamente prescriptivo.

En vez de formular juicios definitivos en cuanto al fondo de diferentes derechos e intereses, el Grupo de trabajo insiste en el *papel crucial de la prueba de sopesamiento* en la valoración del artículo 7, letra f). Es necesario mantener la flexibilidad de la prueba, pero la manera en que se lleve a cabo debe ser más eficaz en la práctica y debe permitir un cumplimiento más efectivo. Esto deberá traducirse en una *mayor* obligación de *rendición de cuentas* por parte de los responsables del tratamiento, de manera que estos asuman la responsabilidad de *demostrar* que su interés prevalece sobre los intereses y los derechos del interesado.

Directrices y responsabilidad

Para lograr este objetivo, el Grupo de trabajo recomienda que se faciliten directrices en la propuesta de Reglamento del siguiente modo:

1) Resultaría útil identificar y facilitar en un considerando una lista no exhaustiva de factores clave que deban considerarse al efectuar la prueba de sopesamiento, tales como la naturaleza y la fuente del interés legítimo, la repercusión para los interesados y las garantías adicionales que el responsable del tratamiento pueda aplicar para impedir cualquier impacto indebido sobre los interesados. Estas garantías podrán comprender, entre otras:
   - la separación funcional de los datos, el uso adecuado de técnicas de anonimización, el cifrado y otras medidas técnicas y organizativas que limiten los riesgos potenciales para los interesados;
   - pero también medidas que garanticen un aumento de la transparencia y de la libertad de elección de los interesados, tales como, cuando así proceda, la posibilidad incondicional de exclusión voluntaria del tratamiento, gratuita y de manera que se pueda recurrir a ella fácil y eficazmente.

2) El Grupo de trabajo también apoyaría una mayor clarificación en la propuesta de Reglamento sobre el modo en que el responsable del tratamiento puede *demostrar*[111] una mayor rendición de cuentas.

[111] Dicha demostración debe seguir siendo razonable y centrarse en el resultado en vez de en el proceso administrativo.

El cambio de las condiciones para que los interesados ejerzan el derecho de oposición previsto en el artículo 19 de la propuesta de Reglamento constituye ya un importante elemento de responsabilidad. Si el interesado se opone al tratamiento de sus datos en virtud del artículo 7, letra f), de conformidad con la propuesta de Reglamento, competerá al responsable del tratamiento demostrar que su interés prevalece. Esta inversión de la carga de la prueba cuenta con el firme apoyo del Grupo de trabajo, ya que contribuye a la obligación de una mayor rendición de cuentas.

Si el responsable del tratamiento de datos no consigue demostrar al interesado en un caso específico que su interés prevalece, esto puede tener también otras consecuencias en el tratamiento en su conjunto, no solo en relación con el interesado que se opuso. Como resultado, el responsable del tratamiento puede cuestionar o decidir reorganizar el tratamiento cuando resulte apropiado, en beneficio no solo del interesado específico sino también de todos los interesados que se encuentren en una situación similar[112].

Este requisito es necesario pero no suficiente. Con el fin de garantizar la protección desde el principio, y para impedir que se eluda la inversión de la carga de la prueba[113], es importante que se adopten medidas *antes* de que comience el tratamiento, y no solo en el transcurso de los procedimientos de «oposición» posteriores.

Por tanto, se propone que, en la primera fase de cualquier actividad de tratamiento, el responsable del mismo adopte varias medidas. Las dos primeras medidas podrían figurar en un considerando de la propuesta de Reglamento y la tercera en una disposición específica:

- Realizar una evaluación[114], que deberá incluir las diferentes etapas del análisis presentado en este Dictamen y resumido en el anexo 1. El responsable del tratamiento

112 Además de invertir la carga de la prueba, el Grupo de trabajo también apoya que la propuesta de Reglamento no exija ya que la oposición se haga basándose en «razones legítimas [apremiantes] propias de [la] situación particular» [del interesado]. Por el contrario, de conformidad con la propuesta de Reglamento, sería suficiente la referencia a cualesquiera razones legítimas (no necesariamente «apremiantes») relacionadas con la situación particular del interesado. De hecho, otra opción, que se propuso en el Informe final de la Comisión LIBE es suprimir el requisito de que la oposición deba estar relacionada con la situación particular del interesado. El Grupo de trabajo apoya este enfoque en el sentido de que recomienda que los interesados puedan beneficiarse de una o ambas posibilidades, según proceda, es decir, oponerse bien basándose en su situación particular, bien con un carácter más general y, en este último caso, sin que se les exija ninguna justificación específica. Véase en este sentido la enmienda 114 al artículo 19, apartado 1, de la propuesta de Reglamento en el Informe final de la Comisión LIBE.

113 Los responsables del tratamiento, por ejemplo, pueden caer en la tentación de evitar una demostración de que su interés prevalece caso por caso, utilizando formularios de justificación normalizados, o pueden hacer que el ejercicio del derecho de oposición de otro modo devenga engorroso.

114 Esta valoración, tal como se afirmó previamente en el pie de página 84, no deberá confundirse con una evaluación del impacto relativo a la protección de datos y a la intimidad más exhaustiva. En la actualidad, no existen directrices pormenorizadas sobre las evaluaciones de impacto a escala europea, aunque en algunos ámbitos, en concreto para RFID y medición inteligente, se han realizado una serie de loables esfuerzos para definir la metodología o el marco (o el modelo) específico del sector que podría aplicarse en toda la Unión Europea. Véase «*Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications*» («Propuesta de la industria para un marco de evaluación del impacto relativo a la protección de datos y a la intimidad para las aplicaciones basadas en la identificación por radiofrecuencia (RFID)») y «*Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems*» («Modelo de evaluación del impacto relativo a la protección de datos para redes inteligentes y para sistemas de medición inteligentes») elaborado por el Grupo de expertos 2 del Grupo

deberá exponer de manera explícita el interés o intereses en juego que prevalecen y las razones por las que prevalecen sobre los intereses de los afectados. Dicha evaluación preliminar no deberá ser demasiado onerosa, y deberá seguir siendo *modulable*: podrá limitarse a criterios esenciales si el impacto del tratamiento sobre los interesados es insignificante *prima facie*, mientras que deberá realizarse más minuciosamente si resultara difícil alcanzar el equilibrio y este requiriera, por ejemplo, la adopción de varias garantías adicionales. Cuando así proceda —es decir, cuando una operación de tratamiento presente riesgos específicos para los derechos y libertades de los interesados— deberá realizarse una evaluación del impacto relativo a la protección de datos y a la intimidad más exhaustiva (de conformidad con el artículo 33 de la propuesta de Reglamento), de modo que la valoración en virtud del artículo 7, letra f), podría convertirse en una parte importante de la misma.

- Documentar la evaluación. Al igual que es *modulable* la minuciosidad con la que debe llevarse a cabo la evaluación, la cantidad de documentación debe abordarse con el mismo criterio. Dicho esto, deberá facilitarse alguna documentación básica en todos los casos, con la única excepción de los más triviales, independientemente de la valoración del impacto del tratamiento sobre la persona. Sobre la base de dicha documentación se podrá evaluar y, en su caso, impugnar posteriormente la valoración realizada por el responsable del tratamiento.

- Dar transparencia y visibilidad a esta información destinada a los afectados y otras partes interesadas. La transparencia deberá garantizarse tanto respecto de los interesados como respecto de las autoridades de protección de datos y, cuando así proceda, respecto del público en general. En lo que se refiere a los interesados, el Grupo de trabajo se remite al Proyecto de informe de la Comisión LIBE[115], que afirma que el responsable del tratamiento deberá informar al interesado sobre las razones por las que cree que sus intereses prevalecen sobre los intereses o los derechos y libertades fundamentales del interesado. Dicha información deberá facilitarse a los interesados, desde el punto de vista del Grupo de trabajo, junto con la información que el responsable del tratamiento deba facilitar de conformidad con los artículos 10 y 11 de la presente Directiva (artículo 11 de la propuesta de Reglamento). Esto permitirá la posibilidad de oposición por parte del interesado en una segunda fase, y una justificación adicional caso por caso de los intereses que prevalecen realizada por el

---

especial sobre redes inteligentes de la Comisión. El Grupo de trabajo ha emitido en repetidas ocasiones dictámenes en relación con ambas metodologías.
Además, ha habido varias iniciativas para definir la metodología genérica de la evaluación del impacto relativo a la protección de datos, de la que podrán beneficiarse las iniciativas centradas en «sectores específicos». Véase, por ejemplo, el Proyecto PIAF (*A Privacy Impact Assessment Framework for data protection and privacy rights*, Un marco de evaluación del impacto relativo a la protección de los datos y al derecho a la intimidad): http://www.piafproject.eu/.
Además, para directrices a escala nacional, véase, por ejemplo, la metodología de la CNIL (*Commission Nationale de l'Informatique et des Libertés*):
http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Methodology.pdf
y la Guía de evaluación del impacto relativo a la privacidad de la Oficina del Comisario de Información (ICO, en sus siglas en inglés), en:
http://ico.org.uk/pia_handbook_html_v2/files/PIAhandbookV2.pdf.

115 Proyecto de informe sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo 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 (Reglamento general de protección de datos), (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)).

responsable del tratamiento. Además, cuando así se solicite, la documentación en la que se base la evaluación del responsable del tratamiento deberá ponerse a disposición de las autoridades de protección de datos, con el fin de permitir su posible verificación y ejecución, cuando así proceda.

El Grupo de trabajo también apoyaría que estas tres medidas se incluyeran explícitamente en la propuesta de Reglamento tal como se definen previamente. De este modo se reconocería el papel específico de los fundamentos jurídicos en la evaluación de la legitimidad, y se clarificaría la importancia de la prueba de sopesamiento en el contexto más amplio de las medidas de responsabilidad y de las evaluaciones de impacto en el nuevo marco jurídico propuesto.

El Grupo de trabajo considera también aconsejable encargar al Consejo Europeo de Protección de Datos la elaboración de directrices adicionales, cuando así sea necesario, sobre la base del presente marco. Este enfoque daría, al mismo tiempo, suficiente claridad al texto y suficiente flexibilidad a su aplicación.

Anexo 1. Guía rápida sobre cómo llevar a cabo la prueba de sopesamiento del artículo 7, letra f)

Fase 1: Valorar qué fundamento jurídico puede aplicarse potencialmente en virtud del artículo 7, letras a) a f)

El tratamiento de los datos podrá realizarse únicamente si son aplicables uno o más de los seis fundamentos jurídicos contenidos en el artículo 7, letras a) a f) (la misma actividad de tratamiento puede basarse en diferentes fundamentos jurídicos en cada una de las diferentes etapas). Si parece, *prima facie*, que el artículo 7, letra f), puede resultar adecuado como fundamento jurídico, se deberá proceder a la fase 2.

Consejos breves:

- El artículo 7, letra a), se aplica solo si se otorga un consentimiento libre, informado, específico e inequívoco. El hecho de que una persona no se haya opuesto al tratamiento en virtud del artículo 14 no deberá confundirse con el consentimiento del artículo 7, letra a). No obstante, un mecanismo fácil de oposición al tratamiento podrá considerarse como una importante garantía en virtud del artículo 7, letra f).
- El artículo 7, letra b), cubre el tratamiento necesario para la ejecución de un contrato. El hecho de que el tratamiento de los datos esté relacionado con el contrato o previsto de algún modo en las condiciones del contrato no significa necesariamente que este fundamento jurídico sea de aplicación. Cuando así proceda, se deberá considerar el artículo 7, letra f), como una alternativa.
- El artículo 7, letra c), comprende únicamente obligaciones jurídicas claras y específicas en virtud de la legislación de la UE o de un Estado miembro. En caso de directrices no vinculantes (por ejemplo, de agencias reguladoras) o una obligación jurídica de conformidad con la legislación extranjera, se deberá considerar el artículo 7, letra f), como una alternativa.

Fase 2: Calificar un interés como «legítimo» o «ilegítimo»

Para que se considere legítimo, un interés debe cumplir acumulativamente las siguientes condiciones:

- ser lícito (es decir, ser conforme a la legislación nacional y de la UE);
- estar articulado con la claridad suficiente para permitir que la prueba de sopesamiento se realice en contraposición a los intereses y los derechos fundamentales del interesado (es decir, ser suficientemente concreto);
- representar un interés real y actual (es decir, no especulativo).

Fase 3: Determinar si el tratamiento es necesario para conseguir el interés perseguido

Para el cumplimiento de este requisito se deberá considerar si existen otros medios menos invasivos para alcanzar la finalidad prevista del tratamiento y satisfacer el interés legítimo del responsable del tratamiento.

Fase 4: Establecer un equilibrio provisional valorando si los intereses del responsable del tratamiento prevalecen sobre los intereses o los derechos fundamentales de los interesados

Se deberá:

- considerar la naturaleza de los intereses del responsable del tratamiento (derecho fundamental, otro tipo de interés, interés público);
- evaluar el posible perjuicio que el responsable del tratamiento, los terceros o la comunidad en general puedan sufrir si no se realiza el tratamiento de datos;
- tener en cuenta la naturaleza de los datos (¿sensibles en sentido estricto o en sentido amplio?);
- considerar la posición del interesado (menor, empleado, etc.) y del responsable del tratamiento (por ejemplo, si una organización empresarial tiene una posición dominante en el mercado);
- tener en cuenta el modo en que se tratan los datos (a gran escala, prospección de datos, elaboración de perfiles, revelación a un gran número de personas o publicación);
- identificar los intereses o derechos fundamentales del interesado que podrían verse afectados;
- considerar las expectativas razonables de los interesados;
- evaluar las repercusiones para el interesado y compararlas con el beneficio previsto por el responsable del tratamiento.

Consejo breve: Se deberá considerar el efecto del tratamiento real sobre las personas concretas, no debe entenderse como un ejercicio abstracto o hipotético.

Fase 5: Alcanzar un equilibrio final teniendo en cuenta las garantías adicionales

Se deberán identificar y aplicar garantías adicionales adecuadas derivadas del deber de cautela y diligencia, tales como:
- minimización de los datos (por ejemplo, limitaciones estrictas a la recopilación de datos o su eliminación inmediata tras su uso);
- medidas técnicas y organizativas para garantizar que los datos no puedan utilizarse con el fin de adoptar medidas o emprender otras acciones en relación con las personas («separación funcional»);
- uso extensivo de técnicas de anonimización, agregación de datos, tecnologías de protección de la intimidad, protección de la privacidad desde el diseño, evaluaciones del impacto relativo a la intimidad y a la protección de los datos;
- aumento de la transparencia, derecho general e incondicional de oposición (exclusión voluntaria), portabilidad de los datos y medidas relacionadas para capacitar a los interesados.

Consejo breve: El uso de tecnologías y enfoques de protección de la intimidad puede inclinar la balanza a favor del responsable del tratamiento y también proteger a las personas.

Fase 6: Demostrar el cumplimiento y garantizar la transparencia

Se deberá:
- elaborar un plan de cinco fases, de 1 a 5, para justificar el tratamiento antes de su realización;
- informar a los interesados de las razones por las que se cree que la balanza se inclina a favor del responsable del tratamiento;
- conservar la documentación disponible para las autoridades de protección de datos.

Consejo breve: Esta fase es *modulable*: los datos de la evaluación y la documentación deberán adaptarse a la naturaleza y al contexto del tratamiento. Estas medidas serán más amplias cuando se trate una gran cantidad de información sobre muchas personas, de manera que pudiera tener una repercusión significativa para ellas. Una evaluación exhaustiva del impacto relativo a la protección de datos y a la intimidad (en virtud del artículo 33 de la propuesta de Reglamento) será únicamente necesaria cuando la actividad de tratamiento presente riesgos específicos para los derechos y libertades de los interesados. En estos casos, la valoración en

virtud del artículo 7, letra f), podría convertirse en una parte importante de esta evaluación de impacto más amplia.

Fase 7: ¿Qué sucede si el interesado ejerce su derecho de oposición?

- Cuando únicamente se establece un derecho condicionado de exclusión voluntaria como garantía (se exige de manera explícita en virtud del artículo 14, letra a), como garantía mínima): en caso de que el interesado se oponga al tratamiento, deberá garantizarse que existe un mecanismo adecuado y fácil de usar para evaluar de nuevo el equilibrio respecto de la persona afectada e interrumpir el tratamiento de sus datos si esta nueva evaluación demuestra que sus intereses prevalecen.
- Cuando se establece un derecho incondicional de exclusión voluntaria como garantía adicional (bien porque se exige de manera explícita en virtud del artículo 14, letra b), bien porque se considera de otro modo una garantía adicional necesaria o útil): en caso de que el interesado se oponga al tratamiento, deberá garantizarse que se respeta su decisión, sin que se deba realizar otra evaluación o adoptar otra medida.

Anexo 2. Ejemplos prácticos para ilustrar la aplicación de la prueba de sopesamiento del artículo 7, letra f)

El presente anexo ofrece ejemplos relativos a algunos de los contextos más comunes en los que puede surgir la cuestión del interés legítimo en el sentido del artículo 7, letra f). En la mayoría de los casos, se han agrupado dos o más ejemplos relacionados que merece la pena comparar bajo un mismo epígrafe. Muchos de los ejemplos se basan en casos reales o en elementos de casos reales gestionados por las autoridades de protección de datos de los diferentes Estados miembros. No obstante, en ocasiones se han cambiado los hechos en mayor o menor grado para que ayuden a ilustrar mejor cómo llevar a cabo la prueba de sopesamiento.

Estos ejemplos se incluyen con el fin de ilustrar el *proceso de reflexión*: el método que debe utilizarse para llevar a cabo una prueba de sopesamiento teniendo en cuenta diversos factores. En otras palabras, los ejemplos *no* pretenden proporcionar una evaluación *concluyente* de los casos descritos. De hecho, en muchos casos, si se modificasen los hechos del caso de algún modo (por ejemplo, si el responsable del tratamiento adoptara garantías adicionales como una anonimización más completa, mejores medidas de seguridad y más transparencia y posibilidad auténtica de elección por parte de los interesados), el resultado de la prueba de sopesamiento podría cambiar[116].

Esto deberá alentar a los responsables del tratamiento a cumplir mejor todas las disposiciones horizontales de la Directiva y a ofrecer protección adicional, cuando sea pertinente, basada en la privacidad y en la protección de datos desde el diseño. Cuanto más velen los responsables del tratamiento por proteger los datos personales en su conjunto, más probable será que superen la prueba de sopesamiento.

Ejercicio del derecho de libertad de expresión o información[117], incluidas las situaciones en las que se ejerza dicho derecho en los medios de comunicación y en las artes

Ejemplo 1: Una ONG publica de nuevo los gastos de los miembros del Parlamento

Una autoridad pública hace pública, en virtud de la obligación jurídica establecida por el artículo 7, letra c), los gastos de los miembros del Parlamento. Una ONG que vela por la transparencia, a su vez, analiza y vuelve a publicar los datos en una versión precisa y proporcionada, pero más informativa y comentada, contribuyendo a una mayor transparencia y responsabilidad.

Partiendo de la hipótesis de que la ONG lleva a cabo la nueva publicación y su comentario de un modo preciso y proporcionado, adopta las garantías adecuadas y, en general, respeta los

[116] La aplicación correcta del artículo 7, letra f), puede plantear complejas cuestiones de valoración y, con el fin de orientar la evaluación, la legislación específica, la doctrina legal, la jurisprudencia, las directrices, así como los códigos de conducta y otras normas formales o informales, pueden desempeñar un papel fundamental.

[117] Sobre la libertad de expresión o información, véase la página 34 del Dictamen. También deberán tenerse en cuenta cualesquiera excepciones pertinentes, de conformidad con la legislación nacional, al tratamiento con fines periodísticos en virtud del artículo 9 de la Directiva a la hora de valorar estos ejemplos.

derechos de las personas afectadas, deberá poder utilizar el artículo 7, letra f), como fundamento jurídico del tratamiento. Los factores como la naturaleza del interés legítimo (un derecho fundamental de libertad de expresión o información), el interés del público en la transparencia y la responsabilidad y el hecho de que los datos ya hayan sido publicados y hagan referencia a datos personales (relativamente menos sensibles) relacionados con las actividades de las personas que son pertinentes para el ejercicio de sus funciones públicas[118], inclinan la balanza a favor de la legitimidad del tratamiento. El hecho de que la publicación inicial se exigiera por ley y que las personas afectadas deben, pues, esperar que sus datos se publiquen, también contribuye a una valoración favorable. En el otro lado de la balanza, el impacto sobre la persona puede ser significativo. Por ejemplo, debido al escrutinio público, puede cuestionarse la integridad de algunas personas y esto puede dar lugar, llegado el caso, a la pérdida de las elecciones o en algunos casos a una investigación penal por actividades fraudulentas. Los factores anteriores considerados en su conjunto, no obstante, ponen de manifiesto que los intereses del responsable del tratamiento (y los intereses del público al que se revelan los datos) prevalecen sobre los intereses de los interesados.

Ejemplo 2: Un concejal nombra a su hija asistente especial

Un periodista publica un artículo, bien documentado y con una descripción precisa de los hechos, sobre un concejal en un periódico local en línea, que revela que solo ha asistido a una de las últimas once reuniones del ayuntamiento y que es improbable que vuelva a ser reelegido debido a un reciente escándalo sobre el nombramiento de su hija de diecisiete años como asistente especial.

En este caso, se debe aplicar un análisis similar al del *Ejemplo 1*. En cuanto a los hechos, el periódico en cuestión tiene un legítimo interés en publicar la información. Aunque se han revelado datos personales sobre el concejal, el derecho fundamental de libertad de expresión y el derecho a publicar la historia en el periódico prevalecen sobre el derecho a la privacidad del concejal. Esto es así porque el derecho de privacidad de las personalidades públicas es relativamente limitado en relación con sus actividades públicas y debido a la especial importancia de la libertad de expresión, sobre todo cuando la publicación de una historia tiene un interés público.

Ejemplo 3: Los primeros resultados de búsqueda continúan mostrando un delito penal menor

El archivo en línea de un periódico contiene un artículo antiguo relativo a una persona, que fue en tiempos una celebridad local, capitán de un equipo de fútbol de aficionados de un pequeño pueblo. Se identifica a la persona con su nombre completo y la historia relata su implicación en un procedimiento penal relativamente menor (ebriedad y desorden público). La persona en cuestión ya no tiene antecedentes penales y su expediente ya no incluye dicho delito por el que cumplió pena varios años atrás. Lo que resulta más alarmante para la persona es el hecho de que buscando su nombre con los motores de búsqueda comunes en línea, el vínculo a esta noticia antigua está entre los primeros resultados sobre él. Pese a su petición, el

[118] No puede descartarse que algunos gastos puedan revelar datos más sensibles, como datos sanitarios. Si este fuera el caso, estos deberán suprimirse del conjunto de datos antes de su primera publicación. Una buena práctica es adoptar un «enfoque proactivo» y dar a las personas la posibilidad de revisar sus datos antes de su publicación e informarles claramente sobre las posibilidades y modalidades de publicación.

periódico rehúsa adoptar medidas técnicas que restringirían la amplia disponibilidad de la noticia relacionada con el interesado. Por ejemplo, el periódico rehúsa adoptar medidas técnicas y organizativas cuyo objetivo sería, en la medida en que lo permita la tecnología, limitar el acceso a la información desde motores de búsqueda externos utilizando el nombre de la persona como categoría de búsqueda.

Este es otro caso que ilustra el posible conflicto entre la libertad de expresión y la privacidad. También pone de manifiesto que en algunos casos las garantías adicionales —tales como garantizar que, al menos en el caso de una oposición justificada en virtud del artículo 14, letra a), de la Directiva, no pueda accederse ya a la parte pertinente de los archivos del periódico mediante motores de búsqueda externos o que el formato utilizado para mostrar la información no permita la búsqueda por nombre— pueden desempeñar un papel fundamental para conseguir el equilibrio adecuado entre los dos derechos fundamentales afectados. Esto se produce sin perjuicio de cualesquiera otras medidas que puedan adoptarse por los motores de búsqueda o terceros[119].

La prospección convencional y otras formas de comercialización y publicidad

Ejemplo 4: Una tienda de ordenadores publicita productos similares a los clientes

Una tienda de ordenadores obtiene de sus clientes sus datos de contacto en el contexto de la venta de un producto, y los utiliza para publicitar mediante correo ordinario sus propios productos similares. La tienda también vende productos en línea y envía correos electrónicos promocionales cuando se reciben existencias de una nueva línea de productos. Se informa a los clientes claramente de la posibilidad de oponerse, gratuita y fácilmente, cuando se recopilan sus datos de contacto y cada vez que se envía un mensaje, en caso de que el cliente no se opusiera inicialmente.

La transparencia del tratamiento, el hecho del que el cliente puede razonablemente esperar la recepción de ofertas de productos similares como cliente de la tienda y el hecho de que tiene la posibilidad de ejercer el derecho de oposición ayudan a reforzar la legitimidad del tratamiento y a garantizar los derechos de las personas. En el otro lado de la balanza, no parece que haya una repercusión desproporcionada en el derecho a la privacidad de la persona (en este ejemplo se presupone que la tienda de ordenadores no ha creado perfiles complejos de sus clientes, por ejemplo, utilizando un análisis detallado de los datos de navegación por Internet).

Ejemplo 5: Una farmacia en línea lleva a cabo una amplia elaboración de perfiles

Una farmacia en línea realiza campañas de publicidad basadas en las medicinas y otros productos que los clientes han adquirido, incluidos productos obtenidos con receta médica. Analiza esta información, combinada con la información demográfica sobre los clientes (por ejemplo, su edad y género), para elaborar un perfil de «salud y bienestar» de los clientes individuales. También se utilizan los datos de navegación por Internet, que se recopilan no solo sobre los productos que los clientes adquieren sino también sobre otros productos e información que estuvieran buscando en el sitio web. Los perfiles de los clientes incluyen información o predicciones que sugieren que una clienta concreta está embarazada, sufre una

[119] Véase también el asunto C-131/12 Google Spain / Agencia Española de Protección de Datos, en la actualidad ante del Tribunal de Justicia de la Unión Europea.

enfermedad crónica concreta o estaría interesada en adquirir complementos dietéticos, bronceadores u otros productos para el cuidado de la piel en determinadas épocas del año. Los analistas de la farmacia en línea utilizan esta información para ofrecer medicinas sin receta médica, complementos alimenticios y otros productos a personas particulares por correo electrónico.

En este caso, la farmacia no puede invocar su interés legítimo cuando crea y utiliza sus perfiles de cliente para las campañas de publicidad. La elaboración de perfiles descrita plantea varios problemas. La información es especialmente sensible y puede revelar una gran cantidad de datos sobre asuntos que muchas personas esperarían que siguieran siendo privados[120]. El alcance y el modo de elaboración de perfiles (utilización de datos de navegación, algoritmos predictivos) también sugieren un alto grado de intrusismo. No obstante, el consentimiento basado en el artículo 7, letra a), y en el artículo 8, apartado 2, letra a) (cuando están en juego datos sensibles) podría considerarse una alternativa cuando proceda.

Mensajes no comerciales que no hayan sido solicitados, incluidos los pertenecientes a campañas políticas o de recaudación de fondos para organizaciones caritativas

Ejemplo 6: Un candidato hace un uso específico del censo electoral en las elecciones locales

Un candidato utiliza el censo electoral[121] en las elecciones locales para enviar una carta de presentación como promoción de su campaña a las siguientes elecciones a cada votante potencial de su distrito electoral. El candidato utiliza los datos obtenidos del censo electoral únicamente para enviar la carta y no conserva los datos una vez que la campaña finaliza.

Las personas afectadas pueden esperar razonablemente dicho uso del censo local durante un periodo preelectoral: el interés del responsable del tratamiento es claro y legítimo. El uso limitado y concreto de la información también contribuye a inclinar la balanza a favor del interés legítimo del responsable del tratamiento. Dicho uso de los censos electorales puede estar también regulado por la legislación nacional, desde la perspectiva del interés público, ofreciendo normas, limitaciones y garantías específicas respecto al uso del censo electoral. Si este es el caso, se exigirá también el cumplimiento de estas normas específicas para garantizar la legitimidad del tratamiento.

Ejemplo 7: Un organismo sin ánimo de lucro recopila información con fines de publicidad específica

Una organización filosófica dedicada al desarrollo humano y social decide organizar actividades de recaudación de fondos basándose en el perfil de sus miembros. Con este fin, recopila datos sobre los sitios de redes sociales mediante un software *ad hoc* que se centra en personas a las que les «gustó» la página de la organización, les «gustó» o «compartieron» los mensajes que la organización publicó en su página, vieron determinados artículos o

120 Más allá de cualesquiera restricciones impuestas por la legislación de protección de datos, la publicidad de productos con receta médica también está estrictamente regulada en la UE y existen también algunas restricciones relativas a la publicidad de medicamentos sin receta médica. Además, deberán también tenerse en cuenta los requisitos del artículo 8 sobre categorías especiales de datos (como los datos sanitarios).

121 Se presupone que en el Estado miembro en el que se produce la situación de este ejemplo existe un censo electoral establecido por ley.

retuitearon los mensajes de la organización. Después envía mensajes y boletines a sus miembros de acuerdo con sus perfiles. Por ejemplo, los propietarios de perros mayores a los que les «gustaron» artículos sobre refugios de animales reciben diferentes llamamientos de recaudación de fondos de familias con niños pequeños; las personas de diferentes grupos étnicos también reciben mensajes diferentes.

El hecho de que se trate de categorías especiales de datos (creencias filosóficas) exige el cumplimiento del artículo 8, condición que parece cumplirse ya que el tratamiento tiene lugar en el transcurso de las actividades legítimas de la organización. No obstante, esta no es una condición suficiente en este caso: el modo en que se utilizan los datos excede las expectativas razonables de las personas afectadas. La cantidad de datos recopilados, la falta de transparencia sobre la recopilación y la reutilización de los datos inicialmente publicados con un fin diferente lleva a concluir que, en este caso, no puede utilizarse el artículo 7, letra f), como fundamento jurídico. Por tanto, el tratamiento no deberá permitirse excepto si puede utilizarse otro fundamento, por ejemplo, el consentimiento de las personas afectadas en virtud del artículo 7, letra a).

Ejecución de demandas legales, incluido el cobro de deudas mediante procedimientos extrajudiciales

Ejemplo 8: Conflicto sobre la calidad de las obras de renovación

Un cliente cuestiona la calidad de las obras de renovación de su cocina y rehúsa pagar el precio total. La empresa constructora transfiere los datos pertinentes y proporcionados a su abogado con el fin de que exija el pago al cliente y negocie un acuerdo con este en caso de que continúe negándose a pagar.

En este caso, las medidas previas adoptadas por la empresa constructora utilizando la información básica del interesado (por ejemplo, nombre, dirección, referencia del contrato) para enviar un recordatorio al interesado (directamente o mediante su abogado, como en este caso) pueden todavía considerarse dentro del ámbito del tratamiento necesario para la ejecución del contrato (artículo 7, letra b)). No obstante, la adopción de nuevas medidas[122], incluida la participación de una agencia de cobro de deudas, deberá evaluarse en virtud del artículo 7, letra f), teniendo en consideración, entre otros, el intrusismo y el impacto sobre el interesado, tal como se pondrá de manifiesto en el ejemplo siguiente.

Ejemplo 9: Un cliente desaparece con un automóvil adquirido a crédito

Un cliente incumple el pago de los plazos vencidos respecto de un caro automóvil deportivo adquirido a crédito, y después «desaparece». El concesionario contrata a un tercero «agente de cobro». El agente de cobro lleva a cabo una intrusiva investigación «de estilo coercitivo», utilizando, entre otros, prácticas como la videovigilancia encubierta y las escuchas telefónicas.

Aunque los intereses del concesionario y del agente de cobro son legítimos, la balanza no se inclina a su favor debido a los métodos intrusivos utilizados para recopilar la información,

[122] Existe en la actualidad, entre los Estados miembros, una gran variedad de disposiciones sobre qué medidas deben considerarse necesarias para la ejecución de un contrato.

algunos de los cuales están explícitamente prohibidos por ley (escuchas telefónicas). La conclusión sería diferente si, por ejemplo, el concesionario o el agente de cobro solo realizasen comprobaciones limitadas para confirmar los datos de contacto del interesado con el fin de iniciar un procedimiento judicial.

Prevención del fraude, uso indebido de servicios o blanqueo de dinero

Ejemplo 10: Verificación de los datos de los clientes antes de la apertura de una cuenta bancaria

Una institución financiera sigue procedimientos razonables y proporcionados —según directrices no vinculantes de la autoridad de supervisión financiera gubernamental competente— para verificar la identidad de cualquier persona que desee abrir una cuenta. Mantiene registros de la información utilizada para verificar la identidad de la persona.

El interés del responsable del tratamiento es legítimo, el tratamiento de datos afecta únicamente a información limitada y necesaria (práctica normalizada en la industria, que los interesados pueden esperar razonablemente, y recomendada por las autoridades competentes). Se prevén las garantías adecuadas para limitar cualquier impacto desproporcionado e indebido sobre los interesados. Por tanto, el responsable del tratamiento puede utilizar el artículo 7, letra f), como fundamento jurídico. Alternativamente, y en la medida en que se exijan específicamente las medidas adoptadas en la legislación aplicable, podría aplicarse el artículo 7, letra c).

Ejemplo 11: Intercambio de información para la lucha contra el blanqueo de dinero

Una institución financiera, después de ser asesorada por la autoridad competente de protección de datos, aplica procedimientos basados en criterios específicos y limitados para intercambiar datos relativos a un presunto uso indebido de las normas contra el blanqueo de dinero con otras empresas dentro del mismo grupo, con una limitación estricta de acceso, seguridad y prohibición de cualquier reutilización con otros fines.

Por motivos similares a los explicados anteriormente, y dependiendo de los hechos del caso, el tratamiento de datos podría basarse en el artículo 7, letra f). Alternativamente, y en la medida en que se exijan específicamente las medidas adoptadas en la legislación aplicable, podría aplicarse el artículo 7, letra c).

Ejemplo 12: Lista negra de drogodependientes agresivos

Un grupo de hospitales crea una lista negra conjunta de personas «agresivas» en búsqueda de drogas, con el objetivo de prohibirles el acceso a todas las instalaciones médicas de los hospitales participantes.

Incluso si el interés de los responsables del tratamiento de mantener las instalaciones seguras es legítimo, tiene que sopesarse en relación con el derecho fundamental de privacidad y otras preocupaciones apremiantes, como la necesidad de no excluir a las personas afectadas de acceso al tratamiento sanitario. El hecho de que se trate de datos sensibles (por ejemplo, datos sanitarios relacionados con la adición a las drogas) también respalda la conclusión de que en este caso es improbable que se pueda aceptar el artículo 7, letra f), como fundamento jurídico

del tratamiento[123]. El tratamiento podría ser aceptable si estuviera, por ejemplo, regulado en una ley que ofreciera garantías específicas (comprobaciones y controles, transparencia, prevención de decisiones automatizadas) para que no dé lugar a discriminación o violación de los derechos fundamentales de las personas[124]. En este último caso, dependiendo de si esta ley específica exige o solo permite el tratamiento, tanto la letra c) como la letra f) del artículo 7 podrían considerarse un fundamento jurídico.

Supervisión de los empleados con fines de seguridad o gestión

Ejemplo 13: Horas de trabajo de los abogados de un bufete utilizadas tanto con fines de facturación como con fines de fijación de primas

El número de horas facturables trabajadas por los miembros de un bufete de abogados se trata tanto con fines de facturación como para la fijación de las primas anuales. El sistema se explica de manera transparente a los empleados que tienen el derecho explícito de expresar su desacuerdo con las conclusiones, tanto en relación con la facturación como en relación al pago de primas, para debatirlo después con sus responsables.

El tratamiento parece necesario para el interés legítimo del responsable del tratamiento, y no parece que haya un modo menos intrusivo de alcanzar el objetivo. El impacto sobre los empleados es también limitado debido a las garantías y procesos previstos. Por tanto, el artículo 7, letra f), podría ser un fundamento jurídico apropiado en este caso. También podría argumentarse en favor del tratamiento para uno o ambos fines que este es también necesario para la ejecución del contrato.

Ejemplo 14: Supervisión electrónica del uso de Internet[125]

El empleador supervisa el uso de Internet por los empleados durante las horas laborales para comprobar que no estén haciendo un uso personal excesivo de la TI de la empresa. Los datos recopilados incluyen cookies y archivos temporales generados en los ordenadores de los empleados, que muestran los sitios web visitados y las descargas realizadas durante las horas laborables. Los datos se tratan sin previa consulta a los interesados y a los representantes del sindicato o del comité de empresa. Las personas afectadas no tienen tampoco información suficiente sobre estas prácticas.

La cantidad y la naturaleza de los datos recopilados representan una intrusión significativa en la vida privada de los empleados. Además de las cuestiones de proporcionalidad, la transparencia sobre las prácticas, íntimamente relacionada con las expectativas razonables de los interesados, es también un importante factor que hay que tener en cuenta. Incluso si el empleador tiene un interés legítimo en limitar el tiempo que dedican sus empleados a visitar sitios web no directamente relacionados con su trabajo, los métodos utilizados no superan la prueba de sopesamiento del artículo 7, letra f). El empleador deberá utilizar métodos menos intrusivos (por ejemplo, limitando la accesibilidad a determinados sitios) que, como buena

123 Deberán también tenerse en cuenta los requisitos del artículo 8 sobre categorías especiales de datos (como los datos sanitarios).

124 Véase el Documento de trabajo sobre las listas negras (WP 65), adoptado el 3 de octubre de 2002.

125 Algunos Estados miembros consideran que alguna supervisión electrónica limitada puede resultar «necesaria para la ejecución de un contrato» y, por tanto, puede basarse en el fundamento jurídico de la letra b) en vez de la letra f) del artículo 7.

práctica, sean debatidos y acordados con los representantes de los empleados y comunicados a los empleados de manera transparente.

Regímenes internos de denuncia de irregularidades

Ejemplo 15: Sistema de denuncia de irregularidades para cumplir con las obligaciones jurídicas de la legislación extranjera

Una sucursal de un grupo de EE.UU. en la UE establece un sistema de denuncia de irregularidades limitado para informar sobre infracciones graves en el ámbito de la contabilidad y las finanzas. Las entidades del grupo están sujetas a un código de buen gobierno que insta a fortalecer los procedimientos de control interno y la gestión de riesgos. Debido a sus actividades internacionales, se exige a la sucursal en la UE que facilite datos financieros fiables a otros miembros del grupo en EE.UU. El sistema está diseñado para cumplir tanto la legislación de EE.UU. como las directrices de las autoridades nacionales de protección de datos de la UE.

Entre otras garantías, se facilita a los empleados directrices claras respecto de las circunstancias en las que deberá utilizarse el sistema, mediante sesiones de formación y otros medios. Se advierte al personal que no haga un mal uso del sistema, por ejemplo, haciendo alegaciones falsas o infundadas contra otros miembros de la plantilla. También se les explica que si prefieren pueden utilizar el sistema de manera anónima o si lo desean pueden identificarse ellos mismos. En este último caso, se informa a los empleados de las circunstancias en las que la información que les identifique será facilitada a su empleador o a otras agencias.

Si se exigiera el establecimiento de este sistema en virtud de la legislación de la UE o de conformidad con la legislación de un Estado miembro de la UE, el tratamiento podría basarse en el artículo 7, letra c). No obstante, las obligaciones jurídicas de la legislación extranjera no pueden calificarse como una obligación jurídica a efectos del artículo 7, letra c), y, por tanto, no podrían legitimar el tratamiento en virtud de dicho apartado. Sin embargo, el tratamiento podría basarse en el artículo 7, letra f), por ejemplo, si existe un interés legítimo en garantizar la estabilidad de los mercados financieros o en luchar contra la corrupción, y siempre que el sistema incluya suficientes garantías, de acuerdo con las directrices de las autoridades reguladoras competentes de la UE.

Ejemplo 16: Sistema «interno» de denuncia de irregularidades sin procedimientos coherentes

Una empresa de servicios financieros decide establecer un sistema de denuncia de irregularidades porque sospecha de la existencia de robos y corrupción extendidos entre su personal y desea alentar a sus empleados para que informen sobre los mismos. Con el fin de ahorrar dinero, la empresa decide gestionar el sistema internamente, con miembros de su departamento de recursos humanos. Con el fin de alentar a los empleados a utilizar el sistema ofrece una recompensa en dinero «sin hacer preguntas» a los empleados cuyas actividades de denuncia de irregularidades den lugar a la detección de conductas impropias y a la recuperación de dinero.

La empresa tiene un legítimo interés en detectar y prevenir el robo y la corrupción. Sin embargo, este sistema de denuncia de irregularidades está tan mal diseñado y tiene tal

carencia de garantías que sus intereses quedan anulados, tanto por los intereses como por el derecho a la privacidad de sus empleados, especialmente de aquellos que puedan ser víctimas de falsas acusaciones hechas solamente con un fin de lucro. El hecho de que el sistema funcione internamente y no de modo independiente es otro problema en este caso, así como la falta de formación y orientación sobre el uso del mismo.

Seguridad física, seguridad de la tecnología de la información y seguridad en la red

Ejemplo 17: Controles biométricos en un laboratorio de investigación

Un laboratorio de investigación científica que trabaja con virus letales utiliza un sistema de entrada biométrico debido al alto riesgo para la salud pública en el caso de que los virus salgan de las instalaciones. Se prevén las garantías adecuadas, incluido el hecho de que los datos biométricos se almacenan en tarjetas personales de los empleados y no en un sistema centralizado.

Incluso si los datos son sensibles en sentido amplio, el tratamiento se realiza en el interés público. Tanto esto como el hecho de que los riesgos de mal uso se reducen mediante las garantías adecuadas hacen que el artículo 7, letra f), constituya un fundamento jurídico apropiado para el tratamiento.

Ejemplo 18: Cámaras ocultas para identificar a visitantes y empleados fumadores

Una empresa hace uso de cámaras ocultas para identificar a empleados y visitantes que fuman en zonas no autorizadas del edificio.

Aunque el responsable del tratamiento tiene un interés legítimo en garantizar el cumplimiento de las normas sobre la prohibición de fumar, los medios utilizados para conseguir este fin son, en general, desproporcionados e innecesariamente intrusivos. Existen métodos menos intrusivos y más transparentes a su disposición (como los sensores de detección de humo y los signos visibles). El tratamiento, por tanto, incumple el artículo 6, que exige que los datos «no sean excesivos» en relación con los fines para los que fueron recopilados o reutilizados. Al mismo tiempo, no superaría probablemente la prueba de sopesamiento del artículo 7.

Investigación científica

Ejemplo 19: Investigación sobre los efectos del divorcio y el desempleo de los padres en el nivel educativo de los niños

De conformidad con un programa de investigación adoptado por el gobierno y autorizado por un comité de ética competente, se lleva a cabo una investigación sobre la relación entre el divorcio, el desempleo de los padres y el nivel educativo de los niños. Aunque no se clasifican como «categorías especiales de datos», no obstante, la investigación se centra en cuestiones que para muchas familias serían consideradas información personal íntima. La investigación permitirá que se ofrezca asistencia educativa especial a niños cuya situación podría, si no fuera así, derivar en absentismo, bajo nivel educativo o desempleo y delincuencia cuando sean adultos. La legislación del Estado miembro en cuestión permite explícitamente el tratamiento de datos personales (que no sean categorías especiales de datos) con fines de investigación, siempre que la investigación sea necesaria para un interés público importante y se lleve a cabo

con las garantías adecuadas, que se detallan minuciosamente en la normativa de aplicación. Este marco jurídico incluye requisitos específicos y también un marco de responsabilidad que permite una evaluación de la legalidad de la investigación caso por caso (si se lleva a cabo sin el consentimiento de las personas afectadas) y medidas específicas para proteger a los interesados.

El investigador dirige unas instalaciones de investigación seguras y se le facilita la información pertinente, en condiciones de seguridad, por parte del padrón de habitantes, los tribunales, las agencias de desempleo y los colegios. El centro de investigación procede a «comprobar» las identidades de las personas, de manera que los registros de divorcio, desempleo y educación puedan vincularse, pero sin revelar las identidades «cívicas» de las personas, por ejemplo, sus nombres y direcciones. Todos los datos originales se borran después irreversiblemente. También se adoptan medidas adicionales para garantizar la separación funcional (es decir, que los datos solo puedan utilizarse con fines de investigación) y reducir así cualquier riesgo adicional de nueva identificación.

Los miembros del personal que trabajan en el centro de investigación reciben una rigurosa formación en seguridad y son personalmente (con toda probabilidad incluso penalmente) responsables de cualquier violación de la seguridad a su cargo. Se adoptan medidas técnicas y organizativas, por ejemplo, para garantizar que el personal que utiliza dispositivos USB no pueda llevarse datos personales de las instalaciones.

El centro de investigación tiene un interés legítimo en llevar a cabo la investigación, sobre la que existe un enorme interés público. También se realiza en el legítimo interés de los organismos de empleo, educativos y otros organismos implicados en el programa, porque les ayudará a planificar y a prestar servicios a aquellos que más los necesitan. Los aspectos de privacidad del programa han sido bien diseñados y las garantías previstas hacen que el interés legítimo de las organizaciones implicadas en la investigación prevalezcan sobre los intereses o los derechos de privacidad de los padres o los niños en cuyos registros se basa la investigación.

Ejemplo 20: Estudio de investigación sobre la obesidad

Una universidad desea llevar a cabo una investigación sobre los niveles de obesidad infantil en varias ciudades y comunidades rurales. A pesar de las dificultades generales para obtener acceso a los datos pertinentes de colegios y otras instituciones, consigue persuadir a unas docenas de profesores para supervisar durante un tiempo a los niños de sus clases que parecen obesos y hacerles preguntas sobre su dieta, sus niveles de actividad física, el uso de juegos de ordenador, etc. Estos profesores también registran los nombres y las direcciones de los niños entrevistados, de manera que se les pueda enviar un bono de música en línea como recompensa por participar en la investigación. Los investigadores compilan después una base de datos de los niños, relacionando los niveles de obesidad con la actividad física y otros factores. Las copias en papel de los cuestionarios de entrevistas completados —de forma que todavía se puede identificar a los niños concretos— se conservan en los archivos de la universidad durante un período de tiempo indefinido y sin las medidas de seguridad adecuadas. Se comparten fotocopias de todos los cuestionarios cuando así se solicita con cualquier estudiante de grado de máster o doctorado de dicha universidad o de universidades asociadas en todo el mundo que muestran un interés en la reutilización de los datos de la investigación.

Aunque la universidad tiene un legítimo interés en llevar a cabo la investigación, hay varios aspectos del diseño de la misma que hacen que este interés quede anulado por los intereses y los derechos de privacidad de los niños. Además de la metodología de la investigación, que carece de rigor científico, el problema se deriva, en especial, de la falta de un enfoque de protección de la intimidad en el diseño de la investigación y del amplio acceso a los datos personales recopilados. En ningún momento se codifican o anonimizan los registros de los niños y no se adoptan otras medidas para garantizar ni la seguridad de los datos ni la separación funcional. No se obtiene un consentimiento válido en virtud del artículo 7, letra a), ni de conformidad con el artículo 8, apartado 2, letra a), y no queda claro que se haya explicado a los niños o a sus padres para qué se utilizarán sus datos personales o con quién se compartirán.

Obligación jurídica de la legislación extranjera

Ejemplo 21: Cumplimiento de los requisitos de la legislación fiscal de un tercer país

Los bancos de la UE recopilan y transfieren datos de algunos de sus clientes para que estos cumplan las obligaciones fiscales de un tercer país. La recopilación y la transferencia se definen y se llevan a cabo con las condiciones y las garantías acordadas entre la UE y el país extranjero en un acuerdo internacional.

Aunque una obligación según la legislación extranjera no puede considerarse en sí misma un fundamento legítimo del tratamiento en virtud del artículo 7, letra c), puede serlo si dicha obligación está incluida en un acuerdo internacional. En este último caso, el tratamiento podría considerarse necesario para el cumplimiento de una obligación jurídica incorporada al marco jurídico interno mediante un acuerdo internacional. Sin embargo, si no estuviera vigente dicho acuerdo, la recopilación y la transferencia deberán evaluarse en virtud de los requisitos del artículo 7, letra f), y podrán considerarse permisibles únicamente si se prevén las garantías adecuadas, tales como las aprobadas por la autoridad de protección de datos competente (véase también el *Ejemplo 15* anterior).

Ejemplo 22: Transferencia de datos sobre disidentes

Cuando así se solicita, una empresa de la UE transfiere datos de residentes extranjeros a un tercer país con un régimen opresivo que desea acceder a los datos de disidentes (por ejemplo, los datos del tráfico de su correo electrónico, el contenido de su correo electrónico, el historial de navegación, o los mensajes privados en redes sociales).

En este caso, a diferencia del ejemplo anterior, no existe ningún acuerdo internacional que permita la aplicación del artículo 7, letra c), como fundamento jurídico. Además, hay varios elementos para pronunciarse en contra de la utilización del artículo 7, letra f), como fundamento jurídico adecuado para el tratamiento. Aunque el responsable del tratamiento puede tener un interés económico en garantizar que cumple con las solicitudes de un gobierno extranjero (de otro modo podría sufrir un trato menos favorable por parte del gobierno del tercer país comparado con el ofrecido a otras empresas), la legitimidad y la proporcionalidad de la transferencia resulta altamente cuestionable en virtud del marco de derechos fundamentales de la UE. La repercusión potencialmente enorme para las personas afectadas (por ejemplo, discriminación, privación de libertad, pena de muerte) hace que prevalezcan, sin duda, los intereses y los derechos de las personas afectadas.

Reutilización de datos que constan en fuentes públicas

Ejemplo 23: Valoraciones de políticos[126]

Una ONG que vela por la transparencia utiliza datos sobre políticos que constan en fuentes públicas (promesas hechas en el momento de su elección y registros de voto reales) para valorarlos basándose en si han mantenido sus promesas.

Incluso si el impacto sobre los políticos afectados puede ser significativo, el hecho de que el tratamiento se base en información pública y en relación con sus responsabilidades públicas hace que, con un claro propósito de reforzar la transparencia y la rendición de cuentas, la balanza se incline en interés del responsable del tratamiento[127].

Niños y otras personas vulnerables

Ejemplo 24: Sitio web de información para adolescentes

Un sitio web de una ONG, que ofrece asesoramiento a los adolescentes en relación con cuestiones como el abuso de drogas, los embarazos no deseados o el abuso del alcohol, recopila datos mediante su propio servidor sobre los visitantes del sitio. Inmediatamente anonimiza estos datos y los transforma en estadísticas generales sobre qué partes del sitio web son más populares entre visitantes procedentes de diferentes regiones geográficas del país.

El artículo 7, letra f), podría utilizarse como fundamento jurídico, incluso si se ven afectados datos relativos a personas vulnerables, porque el tratamiento se realiza en el interés público y se prevén estrictas garantías (los datos se anonimizan inmediatamente y solo se utilizan para la creación de estadísticas), lo que ayuda a inclinar la balanza a favor del responsable del tratamiento.

Soluciones de privacidad desde el diseño como garantías adicionales

Ejemplo 25: Acceso a números de teléfono móvil de usuarios y no usuarios de una aplicación: «comparar y olvidar»

Se tratan datos personales para comprobar si se ha otorgado ya algún consentimiento inequívoco en el pasado (es decir, «comparar y olvidar» como garantía).

Se exige a un promotor de aplicaciones que obtenga el consentimiento inequívoco de los interesados con el fin de tratar sus datos personales: por ejemplo, el promotor de aplicaciones desea acceder al libro completo de direcciones electrónicas de los usuarios de la aplicación para recopilar sus datos, incluidos los números de teléfono móvil de los contactos que no utilizan la aplicación. Con este fin, puede tener que evaluar, en primer lugar, si los propietarios de los números de teléfono móvil en el libro de direcciones de usuarios de la

126 Véase y compárese con el ejemplo 7 anterior.

127 Como en los *Ejemplos 1 y 2*, se presupone que la publicación es precisa y proporcionada: la falta de garantías y otros factores pueden cambiar el equilibrio de los intereses dependiendo de los hechos del caso.

aplicación han otorgado su consentimiento inequívoco (en virtud del apartado del artículo 7, letra a)) para que se traten sus datos.

Para este tratamiento inicial limitado (es decir, acceso de lectura de corto plazo al libro completo de direcciones de un usuario de la aplicación) el promotor de aplicaciones puede utilizar el artículo 7, letra f), como fundamento jurídico, sujeto a garantías. Estas garantías comprenderán medidas técnicas y organizativas que aseguren que la empresa solo utiliza este acceso para ayudar al usuario a identificar cuáles de sus personas de contacto son ya usuarios, y cuáles, por tanto, habían otorgado ya un consentimiento inequívoco en el pasado a la empresa para recopilar y tratar números de teléfono con este fin. Los números de teléfono móvil de los no usuarios podrán solo recopilarse y utilizarse con el objetivo estrictamente limitado de verificar si ya han otorgado su consentimiento inequívoco para que se traten sus datos y deberán eliminarse inmediatamente después.

Combinación de información personal en los servicios web

Ejemplo 26: Combinación de información personal en los servicios web

Una empresa de Internet que presta varios servicios, incluidos los servicios de motor de búsqueda, intercambio de vídeos y creación de redes sociales, desarrolla una política de privacidad que contiene una cláusula que le permite «combinar toda la información personal» recopilada sobre cada uno de sus usuarios en relación con los diferentes servicios que utilizan, sin definir ningún periodo de retención de datos. Según la empresa, esto se hace con el fin de «garantizar la mejor calidad posible del servicio».

La empresa pone a disposición de las diferentes categorías de usuarios algunas herramientas, de manera que puedan ejercer sus derechos (por ejemplo, desactivar la publicidad dirigida, oponerse al establecimiento de un tipo específico de cookies).

Sin embargo, las herramientas disponibles no permiten a los usuarios tener un control efectivo del tratamiento de sus datos: los usuarios no pueden controlar las combinaciones específicas de sus datos entre los diferentes servicios y los usuarios no pueden oponerse a la combinación de datos sobre ellos. En conjunto, existe un desequilibrio entre el interés legítimo de la empresa y la protección de los derechos fundamentales de los usuarios, y el artículo 7, letra f), no deberá utilizarse como fundamento jurídico del tratamiento. Sería más apropiado utilizar el artículo 7, letra a), como fundamento jurídico, siempre que se cumplan las condiciones establecidas para la obtención de un consentimiento válido.