GRUPO DE TRABAJO DEL ARTÍCULO 29 SOBRE PROTECCIÓN DE DATOS

1021/00/ES
WP207

Dictamen 06/2013 sobre datos abiertos y reutilización de la información del sector público (ISP)

Adoptado el 5 de junio de 2013

EL GRUPO DE TRABAJO DE PROTECCIÓN DE LAS PERSONAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES

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

vistos el artículo 29 y el artículo 30, apartado 1, letra a), y apartado 3, de dicha Directiva,

visto su Reglamento interno,

HA ADOPTADO EL PRESENTE DICTAMEN:

I. Introducción

1.1. Revisión de la Directiva ISP

El 26 de junio de 2013, la Unión Europea adoptó la Directiva 2013/37/UE del Parlamento Europeo y del Consejo («Modificación de la Directiva ISP») por la que se modifica la Directiva 2003/98/CE relativa a la reutilización de la información del sector público («Directiva ISP»)[1].

La Directiva ISP tiene por objeto facilitar la reutilización de la información del sector público mediante la armonización de las condiciones de reutilización en toda la Unión Europea y la eliminación de obstáculos innecesarios a la reutilización en el mercado interior.

El primer texto de la Directiva ISP de 2003 armonizó las condiciones de reutilización, pero no exigió a los organismos del sector público que facilitaran datos para su reutilización. La cuestión de facilitar datos para su reutilización era básicamente de carácter facultativo: la decisión se dejaba a la discreción de los Estados miembros y de los organismos del sector público afectados. El resultado de esto fue que muchos organismos del sector público de toda Europa optaron sencillamente por no dejar que su información fuera reutilizada.

En este contexto, uno de los objetivos políticos fundamentales de la modificación de la Directiva ISP es introducir el principio de que toda la información pública (es decir, toda la información en poder del sector público, que está a disposición del público con arreglo a la legislación nacional) pueda ser reutilizada con fines comerciales o no comerciales. En determinados casos se admiten excepciones al ámbito de aplicación de la Directiva ISP modificada, especialmente por motivos de protección de datos[2].

Así pues, la Directiva ISP obliga ahora a los organismos del sector público a permitir la reutilización de toda la información pública que posean. Sin embargo, como se expondrá a continuación, no impone a estos organismos la obligación de divulgar públicamente información personal. Únicamente prevé la reutilización de la información si ya es de acceso público con arreglo a la legislación nacional, e incluso entonces, solamente si dicha reutilización no va en detrimento de las disposiciones de la legislación de protección de datos aplicable.

1 DO L 175 de 27.6.2013, p. 1.

2 Por lo que respecta al ámbito de aplicación de la Directiva ISP modificada y las disposiciones relativas a la protección de datos, véase la sección V.

Otras nuevas disposiciones relevantes de la Directiva ISP modificada amplían el ámbito de aplicación de la Directiva ISP para incluir a las bibliotecas (incluidas las universitarias), archivos y museos.

Habida cuenta de lo anterior, la Directiva ISP modificada tiene la capacidad para aumentar considerablemente el acceso a la información en poder de los organismos públicos.

1.2. Reutilización de la ISP y datos personales

Las iniciativas sobre reutilización de la ISP suelen incluir: i) la disponibilidad de bases de datos enteras, ii) en formato electrónico normalizado, iii) a cualquier solicitante, sin proceso de selección, iv) gratuitamente (o con honorarios reducidos), y v) para fines comerciales o no comerciales sin condiciones (o bajo condiciones no restrictivas, a través de una licencia si procede) [3].

Esto puede aportar beneficios que den lugar a una mayor transparencia y a una reutilización innovadora de la información del sector público. No obstante, esta mayor accesibilidad de la información no está exenta de riesgos.

A fin de minimizar estos riesgos, cuando se trata de datos personales, la legislación sobre protección de datos debe contribuir a orientar el proceso de selección de los datos personales que pueden o no facilitarse para su reutilización y las medidas que deben adoptarse para proteger los datos personales. En todos los casos en los que está en juego la protección de la intimidad y los datos personales, es preciso seguir un enfoque equilibrado. Por una parte, las normas sobre protección de los datos personales no deben constituir un obstáculo injustificado al desarrollo del mercado de la reutilización, y por otra, deben respetar el derecho a la protección de los datos personales y el derecho a la intimidad. Es importante hacer hincapié en que, como concepto, el centro de atención de los datos abiertos es la transparencia y la responsabilidad de los organismos del sector público y el crecimiento económico, y no la transparencia de los ciudadanos.

Al aplicar la Directiva ISP y la legislación sobre protección de datos a la reutilización de los datos personales, un organismo del sector público puede adoptar uno de estos tres diferentes tipos de decisiones:

1. decisión de no facilitar información personal para su reutilización con arreglo a la Directiva ISP;
2. decisión de convertir la información personal en forma anónima (generalmente en datos estadísticos agregados)[4] y facilitar únicamente tales datos despersonalizados para su reutilización;
3. decisión de facilitar información personal para su reutilización (en caso necesario, bajo condiciones específicas y con salvaguardias adecuadas).

[3] Obsérvese que, de conformidad con el artículo 8, apartado 1, de la Directiva ISP modificada, las «condiciones [impuestas mediante una licencia] no restringirán sin necesidad las posibilidades de reutilización y no se usarán para restringir la competencia.»

[4] Por lo que respecta a los conjuntos de datos agregados y anonimizados derivados de los datos personales, véase la sección VI.

II. Objetivo del dictamen

2.1. Orientaciones coherentes y buenas prácticas

El objetivo del presente dictamen es contribuir a garantizar una comprensión común del marco jurídico aplicable y ofrecer orientación coherente y ejemplos de mejores prácticas sobre la manera de aplicar la Directiva ISP (modificada) en lo que respecta al tratamiento de datos personales.

El objetivo del presente dictamen no es intentar armonizar los enfoques nacionales en lo que se refiere al nivel de transparencia, la legislación nacional sobre acceso a los documentos, o la disponibilidad de información con arreglo a la legislación nacional correspondiente. Sin embargo, la legislación nacional de aplicación de la Directiva ISP y la interpretación nacional de la Directiva 95/46/CE[5] por lo que respecta a la reutilización de la ISP difieren a veces en una medida que va más allá de lo que puede ser necesario para hacer frente a la diversidad de regímenes nacionales de acceso y los diferentes niveles de transparencia.

A este respecto, las recomendaciones políticas sobre la intimidad elaboradas en septiembre de 2012 por la red temática LAPSI (*Legal Aspects of Public Sector Information*) ilustran claramente las innecesarias disparidades en la manera en que la Directiva ISP se ha transpuesto al ordenamiento jurídico de los Estados miembros en lo que respecta a la protección de los datos personales[6]. La propia Directiva ISP también advierte de que las incertidumbres y diferencias legislativas podrían acentuarse con el futuro desarrollo de la sociedad de la información, que ya ha supuesto una fuerte intensificación de la explotación transfronteriza de la información[7].

La falta de un enfoque coherente puede debilitar la posición de las personas interesadas. También puede plantear cargas reglamentarias innecesarias para las empresas y otras organizaciones que operan a través de las fronteras y suponer así un obstáculo al desarrollo de un mercado común europeo de la reutilización. Por una parte, los interesados deberán tener la seguridad de que sus datos estarán sistemáticamente protegidos con independencia de su traslado a otro Estado miembro, a efectos de la reutilización. Por otro lado, deben evitarse la fragmentación y la complejidad innecesaria a fin de permitir la libre circulación de datos personales en toda Europa, otro objetivo clave de la Directiva 95/46/CE.

2.2. Necesidad de actualizar el Dictamen 7/2003

La modificación de la Directiva ISP tiene lugar una década después de la adopción de la Directiva ISP en 2003. En aquel momento, el Grupo de trabajo del artículo 29 adoptó un dictamen sobre los problemas de protección de datos relativos a la ISP («Dictamen 7/2003»)[8]. Si bien los principios esenciales expuestos en el Dictamen 7/2003 siguen siendo válidos, los avances tecnológicos y otros

---

5 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).

6 LAPSI es una red temática europea sobre aspectos jurídicos de la información del sector público, fundada por la Comisión Europea, véase http://www.lapsi-project.eu/. La recomendación política está disponible en http://www.lapsi-project.eu/lapsifiles/lapsi_privacy_policy.pdf.

7 Véase el considerando 7.

8 Véase el Dictamen del Grupo de trabajo del artículo 29 de julio de 2003 sobre la reutilización de la información del sector público y la protección de los datos personales - En busca del equilibrio - adoptado el 12 de diciembre de 2003 (WP 83). Véanse también dos dictámenes anteriores relacionados del Grupo de trabajo del artículo 29: Dictamen 3/1999 sobre la información del sector público y la protección de los datos personales, adoptado el 3 de mayo de 1999 (WP20) y Dictamen 5/2001 sobre el Informe Especial del Defensor del Pueblo Europeo, adoptado el 17 de mayo de 2001.

en el ámbito de la ISP y la protección de datos, y en particular los cambios legislativos propuestos en ambos campos, justifican los esfuerzos actuales para actualizar y completar el Dictamen de 2003.

Además, el Dictamen puede también tener en cuenta ahora otros esfuerzos recientes y en curso que proporcionan orientación, en particular:

- el Dictamen del Supervisor Europeo de Protección de Datos (SEPD) de 18 de abril de 2012 relativo al Paquete de medidas sobre datos abiertos de la Comisión[9];
- el Dictamen 3/2013 del Grupo de trabajo del artículo 29 en materia de limitación de la finalidad[10];
- los trabajos en curso del subgrupo de tecnología del Grupo de trabajo del artículo 29 sobre técnicas de anonimización[11];
- los trabajos en algunos Estados miembros sobre anonimización y evaluación del riesgo[12]; y
- la jurisprudencia y la práctica existentes sobre el equilibrio entre reutilización y protección de los datos personales en algunos Estados miembros[13].

III. Enfoque y estructura del Dictamen

El Dictamen 7/2003 se centró en el principio de limitación de la finalidad[14], pero también abordó otras cuestiones como los motivos lícitos para la revelación pública y la reutilización de la ISP, la protección especial prevista para los datos sensibles, las transferencias hacia terceros países, la calidad de los datos y los derechos de los interesados. Estas observaciones siguen siendo válidas. Considerando los trabajos anteriores ya realizados, el presente Dictamen se limita a actualizar y completar las conclusiones del Dictamen 7/2003 en caso necesario, a la luz de la evolución legislativa y tecnológica.

La sección IV contribuye a aclarar que la obligación de reutilización en virtud de la Directiva ISP modificada se entiende sin perjuicio de los requisitos de protección de datos, y hace hincapié en la importancia de la «protección de los datos desde el diseño y por defecto» y de las «evaluaciones de impacto de la protección de datos» para garantizar que los problemas sobre protección de datos se abordan antes de que los datos personales se faciliten para su reutilización.

La sección V proporciona orientación, mediante ejemplos ilustrativos, sobre el tipo de datos personales que pueden entrar en el ámbito de aplicación de la Directiva ISP.

La sección VI se refiere a las situaciones que actualmente son más comunes en las iniciativas de reutilización de la ISP: cuando los datos estadísticos agregados, derivados de los datos personales, se

---

[9] Dictamen del SEPD de 18 de abril de 2012 relativo al «Paquete de medidas sobre datos abiertos» de la Comisión Europea, en el que se incluye la propuesta de Directiva por la que se modifica la Directiva 2003/98/CE relativa a la reutilización de la información del sector público (ISP), una Comunicación sobre datos abiertos y una Decisión 2011/833/UE de la Comisión relativa a la reutilización de los documentos de la Comisión. Disponible en:

http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-04-18_Open_data_ES.pdf.

[10] Dictamen del Grupo de trabajo del artículo 29 de marzo de 2013 sobre limitación de la finalidad, adoptado el 2 de abril de 2013 (WP 203).

[11] Se espera que se adopte un dictamen a este respecto en el segundo semestre de 2013.

[12] Véase, por ejemplo, el código de prácticas de la anonimización «*Anonymisation: Managing data protection risk code of practice*» publicado por la oficina del Comisario de Información en el Reino Unido en noviembre de 2012 y las directrices sobre análisis de riesgo publicadas por el organismo francés sobre protección de datos en junio de 2012.

[13] Véase, por ejemplo, la Recomendación política de la LAPSI de septiembre de 2012 (pp. 4-14).

[14] Véase el artículo 6, apartado 1, letra b), de la Directiva 95/46/CE.

facilitan de forma agregada y anónima. Como ejemplos cabe citar los datos estadísticos agregados sobre índices de delincuencia, gasto público o rendimiento escolar de los niños en distintas regiones geográficas o en distintos centros de enseñanza. Al ser esta la hipótesis más frecuente de reutilización de la información del sector público que contiene datos personales, una parte importante del Dictamen se dedicará a ella. La principal preocupación en este caso es garantizar la agregación y anonimización efectivas y minimizar el riesgo de que los datos personales puedan ser reidentificados a partir de las series de datos agregados.

La sección VII, con menor grado de detalle, aborda las situaciones en que los datos personales se ponen a disposición del público y, por tanto, pueden estar potencialmente disponibles para su reutilización. Aunque actualmente no es este el escenario típico de las iniciativas de reutilización de la ISP, es importante tener en cuenta que los organismos del sector público cada vez ponen más datos personales a disposición del público, a menudo en internet. Muchas veces se trata de datos personales directamente identificables como, por ejemplo, la información recogida en un registro catastral sobre quién posee un bien inmueble concreto, declaraciones de intereses o salarios de algunos funcionarios o gastos de diputados. Aquí se plantea la cuestión de saber en qué medida, para qué fines, en qué condiciones y con qué salvaguardias pueden facilitarse estos datos para su reutilización. También es importante dejar claro si estos datos están cubiertos por las disposiciones de la Directiva ISP.

En este contexto, es importante destacar que toda información relativa a una persona física identificada o identificable, ya esté a disposición del público o no, constituye datos personales. Por tanto, el acceso y la reutilización de datos personales que se han puesto a disposición del público (por ejemplo, mediante la publicación de los datos en internet) permanecen sujetos a legislación de protección de datos aplicable.

Otras situaciones específicas, como el caso de los datos de investigación y la situación de los archivos históricos, que ahora entran en el ámbito de aplicación de la Directiva ISP, se abordarán brevemente en las secciones VIII y IX.

La sección X aborda la cuestión de la concesión de licencias de la ISP y la necesidad de integrar una cláusula de protección de datos en las licencias, siempre que sea pertinente.

Por último, la sección XI establece una serie de conclusiones y recomendaciones.

IV. No todos los datos personales «a disposición del público» deben facilitarse para su reutilización

4.1. La obligación de reutilización al amparo de la Directiva ISP se entiende sin perjuicio de los requisitos de protección de datos

La Directiva ISP, cuando se adoptó en 2003, no impuso a los organismos del sector público la obligación de autorizar la reutilización de la ISP. La decisión de autorizar o no la reutilización correspondía a los Estados miembros o al organismo del sector público en cuestión (con sujeción al marco regulador nacional sobre transparencia y acceso). El Dictamen 7/2003 se adoptó a la luz de esta «inexistencia de obligación». La sección 2 (cc) del Dictamen 7/2003 establece que «es importante destacar que no se puede invocar la Directiva sobre reutilización como obligación jurídica que hay que cumplir, ya que dicha Directiva no genera ninguna obligación de difusión de información personal».

Con la modificación de la Directiva ISP, el análisis se vuelve más complejo, pero la conclusión final sigue siendo la misma.

El artículo 3, apartado 1, de la Directiva ISP establece que «sin perjuicio de lo dispuesto en el apartado 2, los Estados miembros velarán por que los documentos a los que se aplica la presente Directiva, de conformidad con el artículo 1, puedan ser reutilizados para fines comerciales o no comerciales de conformidad con las condiciones establecidas en los capítulos III y IV». A menos que la reutilización pueda denegarse por las razones que figuran en el artículo 1 (razones derivadas de los regímenes nacionales de acceso y específicamente también por motivos de protección de datos personales), debe autorizarse la reutilización.

Al mismo tiempo, el considerando 21 de la Directiva ISP observa que la Directiva ISP «se debe incorporar al Derecho interno y aplicar de forma que se cumplan plenamente los principios relativos a la protección de los datos personales». Además, el artículo 1, apartado 4, dispone que la Directiva ISP «no menoscaba ni afecta en modo alguno el nivel de protección de las personas físicas en lo que respecta al tratamiento de datos personales».

Estas disposiciones, en conjunto, en una lectura combinada, significan que el «principio de reutilización» no es automático cuando está en juego el derecho a la protección de los datos personales, y no anula las disposiciones aplicables de la normativa sobre protección de datos. Cuando los documentos en poder de los organismos del sector público contienen datos personales, su reutilización está incluida en el ámbito de aplicación de la Directiva 95/46/CE y, por tanto, está sujeta a la normativa sobre protección de datos aplicable.

Por tanto, en los casos en que la reutilización incluye datos personales, el organismo del sector público no puede invocar sistemáticamente la necesidad de cumplir con la Directiva ISP como razón legítima para facilitar datos para su reutilización[15].

4.2. Importancia de una evaluación de impacto de la protección de datos antes de la apertura de los datos para su reutilización

Teniendo en cuenta los riesgos potenciales de la reutilización de la ISP, y, en particular, el hecho de que, una vez que los datos personales se han puesto a disposición del público para su reutilización, será muy difícil controlar eficazmente la utilización de estos datos, el Grupo de trabajo del artículo 29 hace hincapié en la necesidad de respetar los principios de «protección de datos desde el diseño y por defecto» y de garantizar que las cuestiones de protección de datos se abordan en una fase temprana. En particular, el Grupo recomienda encarecidamente la realización de un análisis de impacto exhaustivo sobre la protección de datos por el organismo del sector público antes de facilitar datos personales para su reutilización. Los Estados miembros han de estudiar también la posibilidad de hacer tal evaluación de impacto obligatoria en virtud de la legislación nacional, o de promoverla como buena práctica. En cualquier caso, incluso si ello no está expresamente previsto en la legislación nacional, antes de divulgar la información y de decidir si se facilita para su reutilización, los organismos del sector público deben llevar a cabo una evaluación exhaustiva para determinar si los datos personales pueden facilitarse para su reutilización y, en caso afirmativo, en qué condiciones y con qué garantías específicas sobre protección de datos puede permitirse la reutilización.

[15] El Grupo de trabajo también pretende dejar claro que, desde la perspectiva de quien reutiliza los datos, la Directiva ISP en sí misma no crea un motivo legítimo para el tratamiento. (Por lo que respecta a los motivos legítimos, véase el Dictamen 7/2003 así como la sección 7.5 del presente Dictamen.)

La evaluación debería, entre otras cosas, determinar una base jurídica para la divulgación (y la potencial base jurídica para la reutilización), evaluar los principios de limitación de la finalidad, proporcionalidad y minimización de datos, y considerar la protección particular que requieren los datos sensibles. Para llevar a cabo esta evaluación, deberá analizarse detenidamente el potencial impacto sobre los interesados.

Esta evaluación debe ayudar a decidir qué datos personales, en su caso, pueden facilitarse para su reutilización, y con qué garantías[16]. Cabe destacar que la propuesta de Reglamento de protección de datos[17] fomenta y en algunos casos exige que se realicen evaluaciones del impacto sobre la protección de datos como instrumento fundamental para contribuir a garantizar la responsabilidad de los responsables del tratamiento de datos[18].

Siempre que sea posible, el análisis previo a la decisión de reutilización debería basarse en un debate informado y la representación de distintas partes interesadas, incluido el responsable del tratamiento que desee facilitar los datos y las partes que requieran los datos y que, por tanto, pueden proporcionar contexto para el debate, así como los representantes de las personas cuyos datos personales están en juego (por ejemplo, organizaciones de defensa del consumidor, organizaciones de derechos de los pacientes, o sindicatos de profesores). Cuando el resultado no esté claro, la autoridad de protección de datos competente y las autoridades nacionales responsables de la libertad de información podrán ofrecer orientación.

Asimismo, los Estados miembros deben examinar la posibilidad de establecer y proporcionar apoyo a redes de conocimientos y centros de excelencia, permitiendo así la puesta en común de buenas prácticas relativas a los datos abiertos y la anonimización. Ello puede revestir particular importancia para organismos del sector público más pequeños que pueden carecer de las competencias necesarias para llevar a cabo la anonimización, una evaluación de impacto de la protección de datos y para evaluar y probar los riesgos de reidentificación[19].

---

[16] En caso de que la evaluación lleve a la decisión de no facilitar para su reutilización datos personales como tales, sino facilitar conjuntos de datos anonimizados derivados de datos personales, debería realizarse un análisis de riesgo sobre la reidentificación. Véase la sección VI sobre anonimización y evaluación de riesgo de la reidentificación.

[17] El 25 de enero de 2012, la Comisión adoptó un paquete de reforma del marco europeo de protección de datos. El paquete incluye: i) una Comunicación [COM(2012)9 final], ii) una propuesta de Reglamento sobre protección de datos [COM(2012)11 final], y iii) una propuesta de Directiva sobre protección de datos [COM(2012)10 final].

[18] Para mayor orientación sobre cómo realizar una evaluación de impacto en materia de protección de datos, véase, por ejemplo, el sitio web del proyecto PIAF (*A Privacy Impact Assessment Framework for data protection and privacy rights*) en la siguiente dirección: http://www.piafproject.eu/Index.html. PIAF es un proyecto cofinanciado por la Comisión Europea que aspira a fomentar que la UE y sus Estados miembros adopten una política progresiva de evaluación de impacto sobre la intimidad como forma de abordar necesidades y retos relacionados con la intimidad y el tratamiento de los datos personales. También hay orientación disponible en algunos Estados miembros. Véase, por ejemplo, el manual relativo a la evaluación de impacto sobre la intimidad publicado por el comisario de información del Reino Unido, en la siguiente dirección: http://ico.org.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment; las directrices sobre análisis de riesgo publicadas por la autoridad francesa de protección de datos, ya mencionadas en la nota 12, y la orientación proporcionada por el comisario de información esloveno, específicamente sobre «Evaluaciones de impacto sobre la intimidad en los proyectos de la administración electrónica», en: https://webmail.europarl.europa.eu/exchweb/bin/redir.asp?URL=https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/PIASmernice__ENG_Lektorirano_10._6._2011.pdf.

[19] Como ejemplo, en el Reino Unido un consorcio liderado por la Universidad de Manchester, junto con la Universidad de Southampton, la oficina nacional de estadística y el nuevo Open Data Institute (ODI) del Estado, opera la red UKAN (UK Anonymisation Network) a fin de permitir compartir buenas prácticas sobre anonimización en los sectores público y privado. La red consta de un sitio web en la siguiente dirección: https://webmail.europarl.europa.eu/exchweb/bin/redir.asp?URL=http://www.ukanon.net, así como de estudios de casos, consultorios y seminarios.

Por último, también se recomienda encarecidamente realizar una evaluación de impacto antes de adoptar nuevas normativas que impliquen la divulgación de datos personales.

V. Ámbito de aplicación de la Directiva ISP: excepciones por motivos de protección de los datos personales

La presente sección proporciona directrices sobre el ámbito de aplicación de la Directiva ISP y, en particular, sobre las excepciones por motivos de protección de datos.

5.1. Aplicabilidad del marco general de protección de datos a la reutilización de la ISP

El considerando 21 de la Directiva ISP observa que «[l]a presente Directiva se debe incorporar al Derecho interno y aplicar de forma que se cumplan plenamente los principios relativos a la protección de los datos personales». Además, el artículo 1, apartado 4, dispone que la Directiva ISP «no menoscaba ni afecta en modo alguno el nivel de protección de las personas físicas en lo que respecta al tratamiento de datos personales».

5.2. Excepciones por motivos de protección de los datos personales

La Directiva ISP establece que «[l]a presente Directiva no se aplicará a: … los documentos a los que no pueda accederse en virtud de regímenes de acceso de los Estados miembros …»[20].

Además, la Directiva ISP modificada también prevé excepciones por motivos de protección de datos. El artículo 1, apartado 2, letra c *quater*, contempla los tres siguientes casos, todos ellos excluidos del ámbito de aplicación de la Directiva ISP:

- los documentos a los que no pueda accederse en virtud de regímenes de acceso por motivos de protección de los datos personales;
- los documentos cuyo acceso esté limitado en virtud de regímenes de acceso por motivos de protección de los datos personales; y
- «las partes de documentos accesibles en virtud de dichos regímenes que contengan datos personales cuya reutilización se haya definido por ley como incompatible con la legislación relativa a la protección de las personas físicas con respecto al tratamiento de los datos personales».

5.3. Observaciones generales

El Grupo de trabajo subraya que, independientemente del «principio de reutilización» formulado en la modificación de la Directiva ISP, la reutilización para fines comerciales o no comerciales de conformidad con las disposiciones de la Directiva ISP no siempre es adecuada en los casos en que la ISP que vaya a ser reutilizada contenga datos personales. Las decisiones relativas a la reutilización de datos personales de conformidad con las disposiciones de la Directiva ISP deberán tomarse caso por caso, y también es preciso establecer medidas legales, técnicas u organizativas adicionales para proteger a las personas interesadas.

La reutilización de los datos personales está y debe estar limitada por:

- disposiciones generales de la legislación aplicable en materia de protección de datos;
- (en su caso) restricciones jurídicas adicionales específicas;

[20] Véase la Directiva ISP, artículo 1, apartado 2, letra c).

- garantías técnicas y organizativas que se hayan establecido para proteger los datos personales.

5.4. Documentos a los que no pueda accederse

Esta disposición excluye del ámbito de aplicación de la Directiva ISP todos los documentos a los que no pueda accederse en virtud de regímenes de acceso del Estado miembro de que se trate por motivos de protección de los datos personales.

A diferencia de la legislación sobre protección de datos, que está armonizada en gran medida sobre la base de la Directiva 95/46/CE, la legislación sobre acceso a la información difiere considerablemente entre los distintos Estados miembros de la UE. Los regímenes de acceso, por lo general, exigen una prueba de equilibrio que compare los intereses protegidos por las normas de protección de datos y de la intimidad con los beneficios de la apertura y la transparencia. Habida cuenta de las divergencias, el resultado de este ejercicio puede diferir en los distintos Estados miembros de la UE. Por ejemplo, las autoridades fiscales de algunos Estados miembros pueden publicar determinadas partes de las declaraciones de la renta de los contribuyentes (con sujeción a medidas jurídicas, técnicas y de organización necesarias para reducir al mínimo los riesgos de una mala utilización), mientras que otro Estado miembro considera que esta información está incluida en la excepción y debe, en general, mantenerse privada.

Dicho esto, 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*[21], que será necesario cerciorarse de que la divulgación sea necesaria y proporcionada al objetivo legítimo perseguido por la legislación.

En todo caso, una vez que los datos personales contenidos en un documento quedan excluidos del acceso en virtud de las leyes del Estado miembro de que se trate (en particular, cuando la legislación nacional en materia de transparencia y apertura no prevé la accesibilidad general de los datos personales en cuestión), quedarán excluidos asimismo del ámbito de aplicación de la Directiva ISP.

A fin de garantizar la seguridad jurídica y la transparencia para con los interesados, es una buena práctica, siempre que sea posible, adoptar un enfoque proactivo y definir de antemano los datos personales que pueden divulgarse. Los interesados podrán entonces ser informados, en el momento de la recogida de los datos, si alguna parte de los datos personales que comunican, o que se tratarán en el curso del procedimiento administrativo, se harán públicos como resultado de la legislación en materia de libertad de información.

5.5. Documentos cuyo acceso esté limitado

Esta disposición excluye del ámbito de aplicación de la Directiva ISP todos los documentos cuyo acceso esté limitado en virtud de regímenes de acceso del Estado miembro de que se trate por motivos de protección de los datos personales. También en este caso, los regímenes de acceso de los distintos Estados miembros pueden variar en cuanto a qué datos pueden ser objeto de limitación de acceso y qué tipo de limitaciones pueden darse. A continuación figuran algunos ejemplos:

[21] Véanse las sentencias del TJ de 20 de mayo de 2003, Rundfunk, asuntos acumulados C-465/00, C-138/01 y C-139/01, y de 9 de noviembre de 2010, Volker und Markus Schecke, asuntos acumulados C-92/09 y C-93/09.

- Fondos de archivos nacionales que contengan datos personales a los que únicamente pueda accederse en condiciones específicas, y salvaguardias adicionales (véase la sección IX).
- Fondos de datos de investigación que contengan datos personales a los que únicamente pueda accederse en condiciones específicas, y salvaguardias adicionales (véase la sección VIII),
- Determinada información de los registros públicos, autos de procedimientos u otros documentos administrativos que contengan datos personales a los que únicamente puedan acceder personas u organizaciones que acrediten un interés legítimo, o a los que únicamente pueda accederse en condiciones específicas, y salvaguardias adicionales.

5.6. Partes de documentos accesibles cuya reutilización sea incompatible

Esta disposición excluye del ámbito de aplicación de la Directiva ISP

- partes de documentos
- accesibles en virtud de regímenes nacionales de acceso
- que contengan datos personales «cuya reutilización se haya definido por ley como incompatible con la legislación relativa a la protección de las personas físicas con respecto al tratamiento de los datos personales».

Esta disposición confirma que, incluso en los casos en que determinados documentos que contienen datos personales sean plenamente accesibles, su reutilización puede, sin embargo, verse limitada por motivos de protección de datos.

El Grupo de trabajo del artículo 29 hace hincapié en que esta disposición de la Directiva ISP debe interpretarse de conformidad con el artículo 1, apartado 4, de la Directiva ISP, que declara que la Directiva ISP «no menoscaba ni afecta en modo alguno el nivel de protección de las personas físicas en lo que respecta al tratamiento de datos personales».

El Grupo de trabajo del artículo 29 acogería con satisfacción como buena práctica la adopción de disposiciones legales específicas en la legislación nacional que describan claramente i) qué datos se divulgan, ii) para qué fines, y iii) si procede, especifiquen en qué medida y bajo qué condiciones se permite la reutilización. No obstante, cuando no existan estas disposiciones específicas, ello no significa que los datos personales que estén a disposición del público puedan siempre reutilizarse con arreglo a la Directiva ISP.

En estos casos, la legislación sobre protección de datos (aplicada junto con otra legislación pertinente, como la relativa al acceso a los documentos) determinará si los datos personales pueden facilitarse para su reutilización en el caso específico, y en caso afirmativo, con qué salvaguardias adicionales. Si el resultado de esta evaluación es positivo, se autorizará la reutilización, con sujeción a garantías específicas sobre protección de datos y a todas las demás condiciones establecidas en la Directiva ISP (siempre que sean sin perjuicio de lo dispuesto en la legislación sobre protección de datos). Si el resultado de la evaluación es negativo, la reutilización quedará fuera del ámbito de aplicación de la Directiva ISP.

Los ejemplos siguientes pueden ayudar a ilustrar cuándo puede aplicarse esta excepción del ámbito de la Directiva ISP. En el primer ejemplo, las limitaciones a la reutilización están claramente establecidas por ley.

- La legislación fiscal de un Estado miembro puede prever que las declaraciones de la renta de todos los residentes del país estén disponibles públicamente para su revisión por cualquier otro residente, previa solicitud en las oficinas de las autoridades fiscales, sin necesidad de

demostrar un interés legítimo. La ley también especifica claramente que los datos no podrán ser tratados posteriormente, por ejemplo, publicarse en internet, combinarse con otros datos o elaborarse en mayor medida. Una ONG solicita el acceso y el derecho a reutilizar la base de datos de la declaración fiscal para su publicación en su sitio web. En este caso, los datos fiscales quedan fuera del ámbito de aplicación de la Directiva ISP y no hay ninguna obligación para el organismo del sector público de facilitar el conjunto de datos para su reutilización en virtud de la Directiva ISP.

En muchos otros casos, sin embargo, es probable que las restricciones legales estén expresadas con menos claridad y sean menos categóricas en cuanto a las condiciones de reutilización. Por lo general, varios registros civiles, mercantiles y de población, y otras bases de datos, permiten la consulta de datos personales por el público, cada vez más en formato digital a través de internet. La accesibilidad está, con frecuencia, sujeta a garantías específicas, en particular restricciones técnicas sobre las funciones de búsqueda y la descarga a granel. Asimismo, puede solicitarse a los usuarios que acepten las condiciones de acceso.

- La legislación fiscal en un Estado miembro podrá prever que los nombres de los residentes que tengan impuestos atrasados por encima de un determinado umbral durante un período de tiempo prolongado se publiquen en un sitio internet específico, durante un período de tiempo limitado, con salvaguardias técnicas adicionales, en particular limitaciones sobre la descarga a granel y las funciones de búsqueda. El objeto de esta publicación es fomentar el pago de los impuestos a tiempo y servir como castigo adicional (en cuanto a la reputación) para quienes no lo hagan. Un consorcio de bancos solicita el acceso para la reutilización, a fin de introducir los datos en su sistema de información sobre créditos.
- Leyes específicas en el sector de la asistencia sanitaria en un Estado miembro pueden autorizar a los pacientes, con sujeción a salvaguardias, a verificar, en un sitio web específico, si un determinado doctor u otro profesional está suspendido del ejercicio profesional. Se aplican salvaguardias técnicas, en particular limitaciones sobre la descarga a granel y las funciones de búsqueda. Una organización de derechos de los pacientes solicita acceso para la reutilización con vistas a la creación de un sitio web multilingüe y de más fácil utilización para acceder a los mismos datos.
- Leyes específicas de un Estado miembro pueden requerir la publicación de los nombres de los donantes a partidos políticos que sobrepasen un determinado umbral. La información que puede revelar la afiliación política de los donantes se publica en un sitio web específico. Se aplican salvaguardias técnicas, en particular limitaciones sobre la descarga a granel y las funciones de búsqueda. Un grupo de activistas solicita acceso a los datos a granel para su reutilización en virtud de la Directiva ISP con vistas a crear un nuevo sitio web con características adicionales y mejores funciones de búsqueda.
- El nombre y dirección del propietario de un bien inmueble es público en el registro de la propiedad de un Estado miembro, pero la búsqueda en la base de datos de acceso público está limitada de manera que solo se puede buscar un bien inmueble determinado y no un individuo determinado. La descarga a granel también está limitada. Una empresa comercial solicita acceso a los datos a granel para su reutilización con vistas a la creación de un sitio web más fácil de utilizar, a un precio más competitivo.
- Los registros mercantiles de los Estados miembros autorizan el acceso público a una amplia gama de datos personales, en particular nombres, direcciones y muestras de firmas de directores, así como información relativa al accionariado de determinadas formas de sociedades. Existen algunas limitaciones de las funciones de búsqueda y del número de entradas que pueden descargarse. La información está disponible a través de un sitio web específico y sujeto al pago de una tasa. Una empresa comercial solicita acceso a los datos a

granel para su reutilización con vistas a la creación de un sitio web que combine información procedente de varios tipos de registros y que ofrezca mayor información a un precio más competitivo.

En todos los casos, el organismo del sector público interesado debe realizar una cuidadosa evaluación de impacto sobre la protección de datos para decidir si pueden facilitarse los datos para su reutilización en la Directiva ISP y, de ser así, si la legislación sobre protección de datos requiere condiciones específicas y salvaguardias. El «principio de reutilización» no es automático, y no puede tener prioridad sobre las disposiciones aplicables de la normativa de protección de datos.

Esta evaluación detallada es tanto más importante dado que, en virtud de la Directiva ISP, el organismo del sector público, en principio, no debe analizar quien es el solicitante concreto que pide acceso para la reutilización. De conformidad con el artículo 10 (No discriminación), «las condiciones que se apliquen para la reutilización de un documento no deberán ser discriminatorias para categorías comparables de reutilización». Asimismo, conformidad con el artículo 11 (Prohibición de los acuerdos exclusivos), «la reutilización de documentos estará abierta a todos los agentes potenciales del mercado... Los contratos o acuerdos de otro tipo entre los organismos del sector público que conserven los documentos y los terceros no otorgarán derechos exclusivos.»

Por consiguiente, al decidir si autorizan o no la reutilización, los organismos del sector público deben tener en cuenta la compatibilidad de permitir la reutilización en virtud de una licencia abierta no solo al solicitante, sino también a cualquiera que pida los datos. Esto requiere un alto nivel de confianza en que ninguno de los reutilizadores potenciales podrá hacer un uso indebido de los datos personales facilitados.

La Directiva ISP no excluye que los términos y condiciones puedan autorizar el tratamiento solo para fines específicos. La cuestión que se plantea al organismo del sector público es por tanto si la reutilización, por cualquier «posible agente del mercado», a estos efectos, es compatible con las finalidades previstas por el organismo del sector público. La potencial reutilización por parte de las entidades financieras de la información sobre el pago de impuestos, por ejemplo, para fines de información crediticia, es pertinente ya que siguen siendo un potencial reutilizador, según el criterio de «cualquier persona». Por tanto, para resolver los problemas de protección de datos y en particular para garantizar el cumplimiento del principio de limitación de la finalidad, el organismo del sector público (o el legislador) deberá poder limitar, en su caso, las finalidades de la reutilización.

VI. Reutilización de conjuntos de datos agregados y anonimizados derivados de los datos personales

6.1. ¿Cuáles son los beneficios de la agregación y la anonimización para la reutilización de la ISP?

Hasta la fecha, las iniciativas sobre reutilización de la ISP lanzadas por los organismos del sector público a través de «portales de datos abiertos» u otras plataformas han tenido generalmente como objetivo facilitar datos agregados y anonimizados para su reutilización, en vez de datos personales como tales. Este planteamiento es más seguro y debe fomentarse.

Las leyes de protección de datos no suelen permitir que los organismos del sector público publiquen datos personales recogidos para otro fin, generalmente administrativo[22]. Por tanto, en estos casos, su

[22] Por supuesto, cuando sea aplicable, la legislación sobre libertad de información puede exigir la divulgación de datos personales, y el interés en la transparencia y la disponibilidad de información en algunas situaciones puede prevalecer

reutilización como parte de las iniciativas de reutilización de la ISP tampoco es posible. En vez de datos personales, se facilitan y deberían facilitarse (en principio) datos estadísticos derivados de los datos personales. Esta es la solución más eficaz para minimizar el riesgo de revelación inadvertida de datos personales. Estas series de datos agregados y anonimizados no deberán permitir la reidentificación de las personas y, por tanto, no deben contener datos personales.

Decidir el nivel de agregación adecuado y las técnicas específicas de anonimización que deben utilizarse es una tarea difícil. Si la agregación y la anonimización no se hacen de manera eficaz, esto entraña el riesgo de que los individuos puedan ser reidentificados a partir de estos conjuntos de datos. Por tanto, la legislación sobre protección de datos tiene un papel importante que desempeñar a la hora de contribuir a determinar el umbral a partir del cual es «seguro» comunicar datos agregados y anonimizados como parte de una iniciativa de la ISP.

La Directiva 95/46/CE establece un alto nivel para el umbral de anonimización

En el presente documento, el término «anonimización» se refiere a los datos que ya no pueden considerarse datos personales de conformidad con el artículo 2, letra a), de la Directiva 95/46/CE. El artículo 2, apartado a) define los «datos personales» como «toda información sobre una persona física identificada o identificable (el "interesado")». Se considerará identificable «toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social»[23].

El considerando 26 de la Directiva 95/46/CE es también pertinente y dispone además que, con el fin de «determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona».

Hay que señalar que ello establece un umbral elevado, como se expondrá más adelante en el presente Dictamen. Salvo que los datos puedan anonimizarse para alcanzar este umbral, sigue siendo aplicable la legislación sobre protección de datos. Esto significa, entre otras cosas, que a menos que se alcance el umbral, la publicación de la información (y cualquier uso posterior) debe ser «compatible» con las finalidades iniciales de la recogida de datos con arreglo al artículo 6, apartado 1, letra b), de la Directiva 95/46/CE. Además, también deberá existir una base jurídica adecuada para el tratamiento en virtud del artículo 7, apartado 2, letras a) a f), de la Directiva 95/46/CE (por ejemplo, el consentimiento, o necesidad de cumplir la ley). En cambio, si los datos han sido anonimizados en el sentido del artículo 2, letra a), y del considerando 26 de la Directiva 95/46/CE, las normas sobre protección de datos dejarán de ser aplicables y los reutilizadores podrán reutilizar los datos sin estas limitaciones.

Una vez más, es preciso hacer hincapié en el hecho de que «datos anonimizados», según el presente Dictamen, son datos que ya no se consideran personales. Los datos anonimizados deben distinguirse, en particular, de los datos que han sido manipulados utilizando diversas técnicas para mitigar los

---

sobre las cuestiones de protección de los datos y la intimidad. Este área en evolución puede aportar cambios en el futuro.

[23] En su declaración de 27 de febrero de 2013 sobre los debates en curso respecto del paquete de reforma de la protección de datos, el Grupo subrayó que una persona física puede considerarse identificable cuando, dentro de un grupo de personas, se la puede distinguir de otros y por tanto tratársela de forma distinta. Esto supone que el concepto de identificabilidad incluye la diferenciación. La declaración también aclara que los números de identificación, datos de localización, direcciones IP, identificadores en línea u otros factores específicos relativos a un individuo deberán considerarse datos personales.

riesgos de reidentificación de los individuos en cuestión, pero que no han alcanzado el umbral establecido en el artículo 2, letra a), y en el considerando 26 de la Directiva 95/46/CE[24]. En muchos supuestos, estas técnicas solo resultan adecuadas para una divulgación limitada a efectos de su reutilización por terceros, pero no para su plena divulgación y reutilización con licencia abierta.

Es también importante hacer hincapié en que una vez que los datos se publican para su reutilización, no habrá control alguno sobre quién puede acceder a ellos. La probabilidad de que «cualquier otra persona» tenga los medios y los utilice para reidentificar a los interesados aumentará considerablemente. Por tanto, y con independencia de la interpretación del considerando 26 en otros contextos, cuando se trata de facilitar datos para su reutilización en virtud de la Directiva ISP, el Grupo de trabajo del artículo 29 desea dejar absolutamente claro que debe tenerse el mayor cuidado en garantizar que los conjuntos de datos facilitados no incluyan datos que puedan ser reidentificados por medios que puedan ser razonablemente utilizados por cualquier persona, incluidos los reutilizadores potenciales, pero también por otras partes que puedan tener interés en obtener los datos, incluidos los servicios con funciones coercitivas.

Más orientación sobre la anonimización y el concepto de datos personales

Para mayor orientación sobre la anonimización y el concepto de datos personales, véase el Dictamen 4/2007 de del Grupo de trabajo del artículo 29 sobre el concepto de datos personales, adoptado el 20 de junio de 2007 (documento WP 136). El Grupo también podrá dar otras orientaciones sobre técnicas de anonimización en un documento aparte, el segundo semestre de 2013.

6.2. ¿Cuáles son los retos y límites de la anonimización para la reutilización de la ISP?

La anonimización es cada vez más difícil de lograr con el avance de las modernas tecnologías informáticas y la disponibilidad de la información de forma ubicua. La reidentificación de las personas es cada vez más común y representa una amenaza en la actualidad[25]. En la práctica, existe una importante zona gris, en la que el responsable del tratamiento de datos puede creer que un conjunto de datos está anonimizado, pero un tercero puede ser capaz de identificar al menos a algunas personas a partir de estos datos, por ejemplo, utilizando otros datos públicos o cualquier otra información de que disponga.

Uno de los principales factores de riesgo es el aumento de la cantidad de datos en línea y fuera de línea, tanto a disposición del público como en manos de organizaciones empresariales, que pueden utilizarse para trazar el perfil de las personas con fines de publicidad comportamental y para un abanico creciente de otros fines. Al cotejarse con la realidad de los «grandes datos» de que ya disponen estas organizaciones, la ISP derivada de los datos personales y facilitada para su reutilización podría aumentar la probabilidad de que los particulares puedan ser identificados o de que sus perfiles pueden verse enriquecidos, a menudo sin que las personas sean conscientes de que esté ocurriendo.

---

[24] La declaración de 27 de febrero de 2013 subraya que cuando sea posible rastrear a un individuo o identificarle (indirectamente) por otros medios, siguen siendo de aplicación las normas sobre protección de datos.

[25] Véase, por ejemplo, «*Transparent Government, Not transparent Citizens*», un informe elaborado por el Gabinete de la Presidencia del Reino Unido por Kieron O'Hara de la Universidad de Southampton en 2011, en el que el autor advierte de la capacidad para identificar a las personas a partir de datos anonimizados utilizando, entre otros, técnicas de «identificación rompecabezas» y declara que no hay soluciones técnicas completas para el problema de la desanonimización. El informe está disponible en la siguiente dirección: http://www.cabinetoffice.gov.uk/sites/default/files/resources/transparency-and-privacy-review-annex-b.pdf.
Véase también *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization* de Paul Ohm de la Facultad de Derecho de la Universidad de Colorado, 57 UCLA Law Review 1701 (2010), disponible en línea en: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006.

6.3. ¿Quién debe realizar la agregación y la anonimización, y cuándo?

La agregación y la anonimización deben realizarse en el plazo más breve posible, por el responsable del tratamiento de los datos o por un tercero que actúe por cuenta del responsable del tratamiento o de varios responsables (y que también posea las necesarias cualificaciones especializadas). No puede dejarse que el reutilizador realice la anonimización, por ejemplo como condición para obtener la licencia. Además, es importante garantizar que la posible organización por un tercero de la agregación y la anonimización no genere un conflicto de intereses y garantice que los datos personales solo se utilizarán para realizar la anonimización y se establezcan las garantías necesarias a tal efecto. El tercero también deberá poder asegurar que los datos personales de los que derivan los conjuntos de datos agregados y anonimizados se suprimirán en cuanto ya no sean necesarios a tal efecto.

6.4. Evaluación de los riesgos de la reidentificación

Salvo que los datos puedan ser anonimizados en el sentido del artículo 2, letra a), y del considerando 26 de la Directiva 95/46/CE, la legislación sobre protección de datos sigue siendo aplicable.

Los responsables del tratamiento deben evaluar si una persona puede ser razonablemente identificada a partir del conjunto de datos «anonimizado» que se facilitará para la reutilización, y de otros datos; es decir, si una organización o persona física puede identificar a un individuo a partir de los datos que se facilitan, bien por sí mismos o en combinación con otra información disponible.

Tal como se explica en la sección 6.1, el presente Dictamen no tiene por objeto proporcionar una orientación amplia y concluyente sobre cómo evaluar los riesgos de reidentificación. Tampoco pretende proporcionar una definición concluyente de la «anonimización» o los «datos anonimizados». No obstante, reitera que el lector podrá encontrar más información en documentos existentes (incluidos los mencionados en el punto 6.1) y que también hay trabajos en curso en el subgrupo de tecnología del Grupo de trabajo del artículo 29 sobre técnicas de anonimización, como se ha indicado en la sección 6.1 y en la sección 2.2.

Dicho esto, y sin ánimo de exhaustividad, el Grupo de trabajo del artículo 29 desea destacar algunos de los factores y conceptos que es útil considerar al evaluar los riesgos de reidentificación, en particular:

- qué otros datos están disponibles, bien para el público, o para otras personas u organizaciones; y si los datos que van a publicarse podrían vincularse con otros conjuntos de datos;
- la probabilidad de que se intente la reidentificación (algunos tipos de datos son más atractivos para potenciales intrusos que otros); y
- la probabilidad de que, si se intenta, la reidentificación tenga éxito, teniendo en cuenta la eficacia de las técnicas de anonimización propuestas[26].

¿Qué «otra» información está disponible?

Al determinar si una persona puede ser indirectamente identificada, es necesario analizar si es posible realizar una identificación a partir de los datos en cuestión (en nuestro caso, el conjunto de

[26] Respecto a las técnicas de anonimización, véase el próximo Dictamen del Grupo de trabajo del artículo 29 sobre este tema específico.

datos «anonimizados»), o a partir de esos datos y de *otra información* que esté en posesión, o que pueda estarlo, del organismo o la persona que intente la reidentificación.

La «otra información» necesaria para realizar la reidentificación podría ser información disponible para determinadas empresas u otras organizaciones, incluidas las autoridades con funciones coercitivas u otros organismos del sector público, para determinadas personas o para todo el mundo porque ha sido publicada en internet, por ejemplo. El ejemplo más evidente es el caso en que los datos a disposición del público, como el censo electoral, la guía telefónica u otros datos de fácil acceso buscando en internet, pueden combinarse con los datos (inadecuadamente) «anonimizados», permitiendo la identificación de un individuo (por ejemplo, utilizando su fecha de nacimiento y su código postal).

Los riesgos de reidentificación pueden aumentar si una persona o grupo de personas ya sabe mucho sobre otra persona, por ejemplo, un miembro de la familia, un colega, un contacto en una red social, un médico, un profesor, una agente de un servicio con funciones coercitivas, o cualquier otro profesional.

Lo que importa aquí, sin embargo, no es solo si la persona con conocimiento previo puede identificar al interesado en cuestión, sino si aprenderá algo nuevo de la información obtenida a través de la reidentificación. Los dos ejemplos que figuran a continuación ilustran la importancia de esta distinción.

Ejemplo 1: estadísticas sobre el sarampión. En un caso, los datos estadísticos anonimizados pueden revelar que en la ciudad A en el año 2012, un número X de personas contrajeron el sarampión. No se proporciona mayor información ni un desglose más detallado. Un médico que haya contribuido a las estadísticas facilitando información sobre sus pacientes a las autoridades sanitarias correspondientes posee registros más completos de estos pacientes en su consulta, sujetos al secreto médico. El médico podría reidentificar fácilmente a varios pacientes a partir del conjunto de datos estadísticos. Del mismo modo, una madre que sabe que su hijo contrajo el sarampión ese año podría fácilmente reidentificarlo en el conjunto de datos. No obstante, ni la madre ni el médico aprenderían nada que no supieran ya del conjunto de datos anonimizados que se ha puesto a disposición del público.

Ejemplo 2: alcoholismo y drogadicción, abusos sexuales y rendimiento escolar. Este ejemplo puede compararse con el siguiente. Se realiza una investigación sobre la correlación entre el consumo de drogas y alcohol de los padres, el abuso sexual de niños, y el rendimiento escolar. Se publican datos de investigación supuestamente «anonimizados», con buena intención, pero sin evaluar cuidadosamente los riesgos de reidentificación.

Las estadísticas ponen de manifiesto, entre otras cosas, que en la escuela A, con un total de 500 alumnos matriculados, en el año 2012 el 20 % de los alumnos (100 alumnos) vivía en un hogar en el que al menos uno de sus progenitores es alcohólico o drogadicto. De estos, en el 8 % de los casos (8 alumnos) el niño fue sometido a abusos sexuales. El informe también especifica que ningún otro alumno padeció abusos sexuales en la escuela A.

Además, las cifras muestran que en el 96 % de los casos (96 alumnos) los niños cuyos padres eran alcohólicos o drogadictos tuvieron dificultades en cuanto a su rendimiento escolar («malos resultados» con arreglo a un nivel académico), sin embargo, en este centro solo el 50 % de los alumnos sometidos a abusos sexuales (4) tuvieron dificultades importantes en su rendimiento.

En la escuela es notorio que AA, un alumno brillante y muy trabajador, tiene un entorno familiar problemático, y que su madre es alcohólica. Con frecuencia es objeto de acoso por algunos

compañeros de clase. Estos mismos compañeros de clase detectan ahora a partir de las estadísticas publicadas de nuevo en el boletín de la escuela que AA debe estar incluido en el 50 % de niños víctimas de abusos sexuales que no tienen dificultades en la escuela («buen rendimiento»). Así pues, han obtenido información nueva (y en este caso, muy sensible) a partir de un conjunto de datos anonimizados de manera ineficaz.

El riesgo de combinar información para obtener datos personales aumenta a medida que se desarrollan las técnicas de interrelación de datos y la capacidad informática, y a medida que más información potencialmente «contrastable» está a disposición del público. De hecho, la capacidad informática se duplica cada año y el almacenamiento de datos, debido también a la disponibilidad de los servicios en nube, es probable que se convierta en una mercancía. Por tanto, el riesgo de reidentificación a través de interrelación de datos es imprevisible porque no puede evaluarse con certeza qué datos están ya disponibles o qué datos pueden publicarse en el futuro.

A pesar de la incertidumbre, los riesgos de reidentificación pueden por lo general mitigarse, al menos en cierta medida, respetando el principio de minimización de los datos, es decir, garantizando que solo se facilitan los datos necesarios para un propósito determinado.

Probabilidad de que la reidentificación tenga éxito: prueba del «intruso motivado»

La prueba del «intruso motivado» es un concepto nuevo, que todavía no está plenamente probado. Puede ser útil para determinar si:

- alguien tendría motivación para efectuar la reidentificación, y
- si es probable que la reidentificación tenga éxito.

La prueba del intruso motivado supone esencialmente analizar si un «intruso» sería capaz de lograr la reidentificación *si* estuviera motivado para ello. El «intruso motivado» es una persona (individuo u organización) que desea identificar a la persona de cuyos datos personales se han derivado los datos anonimizados. Esta prueba tiene por objeto determinar si el intruso motivado tendría éxito. El enfoque presupone que el « intruso motivado» es competente y tiene acceso a recursos acordes con la motivación que pueda tener para la reidentificación.

Algunos tipos de datos será más atractivos para un «intruso motivado» que otros. Por ejemplo, un intruso, en general, podría estar más motivado para reidentificar datos personales si tales datos:

- tienen un importante valor comercial (en particular en el mercado negro o fuera de la Unión Europea) y, por tanto, pueden ser comprados y vendidos con fines de lucro[27];
- pueden utilizarse con fines de inteligencia o para su uso por los servicios con funciones coercitivas;
- revelan información sobre personajes públicos de interés periodístico;
- pueden utilizarse con fines políticos o activistas (por ejemplo, como parte de una campaña contra una determinada organización o persona);
- podrían utilizarse por motivos personales malintencionados (por ejemplo, acecho, acoso, intimidación, o meramente para avergonzar a otros);

[27] Esto puede incluir, por ejemplo, datos sobre transacciones u otros datos de comportamiento de los que puedan deducirse perfiles de consumidores individuales, que podrían usarse con fines publicitarios o de discriminación de precios; información financiera u otra que permita la usurpación de identidad; información sensible que pueda utilizarse para chantajear a individuos o para discriminarlos; información médica que puedan utilizar las compañías de seguros, por ejemplo, para denegar la cobertura por razón de una enfermedad preexistente; información que permita deducir la solvencia y que pueda utilizarse para evaluar riesgos de crédito; etc.

- pueden suscitar curiosidad (por ejemplo, el interés de una persona en averiguar quién ha participado en un incidente que figura en un mapa de la delincuencia de su localidad).

Si bien es útil reflexionar sobre las posibles motivaciones de los potenciales intrusos, el Grupo de trabajo del artículo 29 subraya que este enfoque también cuenta con limitaciones considerables:

- el ejercicio puede ser en cierto grado especulativo;
- en ausencia de «factores de motivación» manifiestos como los descritos anteriormente, el ejercicio puede arrojar falsas conclusiones y puede sugerir que datos personales que son relativamente inocuos se faciliten para su reutilización sin necesidad de una anonimización efectiva;
- los intrusos pueden ser complejos e innovadores e «ir por delante», encontrando usos para los datos reidentificados que no se les ocurren a otros;
- con las crecientes tendencias hacia el análisis de «grandes datos», aumenta el riesgo de que, una vez anonimizados, datos en apariencia inocuos puedan, una vez combinados con otra información, entrañar riesgos más graves.

6.5. Prueba de reidentificación

En algunas circunstancias puede ser difícil establecer el riesgo de reidentificación, en particular cuando un tercero pueda utilizar métodos estadísticos complejos para buscar correspondencias entre diferentes datos anonimizados. Por consiguiente, como parte de la evaluación global para determinar el riesgo de reidentificación, es recomendable utilizar la prueba de reidentificación (un tipo de prueba de «cercado» o «penetración») para detectar y abordar las vulnerabilidades frente a la reidentificación. Se trata de intentar reidentificar a personas a partir de los grupos de datos que esté previsto facilitar.

La primera fase de un proceso de prueba de reidentificación debe consistir en hacer inventario de las series de datos que el organismo del sector público ha publicado o se propone publicar. La siguiente fase sería tratar de determinar qué otros datos, personales o no, están disponibles y podrían vincularse a los primeros para dar lugar a una reidentificación. Las «pruebas de penetración» específicas, en particular, deberían contribuir a evaluar cuáles son los riesgos de «identificación rompecabezas», es decir, juntar elementos de información para crear una imagen más completa de una persona.

Por supuesto, la prueba de reidentificación no debe considerarse una panacea y no debe conducir a una falsa sensación de seguridad. En primer lugar, podría resultar difícil realizar la prueba, ya que a menudo se requiere una importante experiencia técnica y herramientas adecuadas, así como conocimientos sobre los demás datos que pueden estar disponibles. En segundo lugar, los responsables del tratamiento de datos también deben ser conscientes de que el riesgo de reidentificación puede variar a lo largo del tiempo. Por ejemplo, ahora se cuenta con técnicas de análisis de datos y herramientas cada vez más potentes y asequibles, y la correspondencia con otros conjuntos de datos es más fácil a medida que se generan más datos. Por tanto, las organizaciones deben efectuar una revisión periódica de su política en materia de divulgación de datos y de las técnicas utilizadas para anonimizarlos. Además, las decisiones nunca deberían basarse únicamente en las amenazas actuales, sino también en futuras amenazas previsibles.

Una vez se ha realizado una evaluación con arreglo a lo expuesto en la sección 6.4 sobre los riesgos de reidentificación y, en caso necesario, tras efectuar una prueba de reidentificación, el organismo del sector público puede determinar si el conjunto de datos puede considerarse o no anonimizado; dicho de otra manera, si ya no contiene datos personales en el sentido del artículo 2, letra a), y del

considerando 26 de la Directiva 95/46/CE. En caso afirmativo, el conjunto de datos podrá facilitarse sin limitaciones en cuanto a la protección de datos[28]. Por otra parte, si la prueba tiene éxito, estos datos no podrán facilitarse (o no podrán seguir facilitándose) como datos anonimizados, sino que deben considerarse datos personales (y, por tanto, su divulgación puede no ser posible, o serlo con sujeción a los requisitos que se examinan en la sección VII).

6.6. Recuperación de los conjuntos de datos comprometidos

En caso de que se demuestre la reidentificación de los datos a partir de un conjunto de datos abiertos, el organismo del sector público que suministre el conjunto de datos deberá poder detener la divulgación o eliminar el conjunto de datos del sitio web donde figuren los datos abiertos. En caso de eliminar la serie de datos del sitio web, el organismo del sector público también deberá informar a los reutilizadores y pedirles que dejen de tratar y que eliminen todos los datos procedentes del conjunto de datos comprometido. Dado que será difícil informar a todos los reutilizadores en el marco de un régimen de licencias abiertas según lo exigido por la Directiva ISP, los organismos públicos deberán aplicar razonablemente medidas efectivas para tratar esta cuestión. Si bien la recuperación puede llegar a menudo demasiado tarde para evitar el daño, es un paso necesario para contribuir a mitigar cualquier impacto negativo sobre los interesados.

VII. Apertura de datos personales para su reutilización

7.1. Ejemplos de datos personales accesibles al público facilitados por organismos del sector público

Si bien la facilitación de conjuntos de datos anonimizados es la hipótesis típica de las iniciativas de reutilización de la ISP, en algunos casos los organismos del sector público también podrán facilitar datos personales para su reutilización.

Muchos registros a disposición del público tales como registros catastrales o registros mercantiles contienen grandes cantidades de datos personales y, debido a las iniciativas de la administración electrónica, cada vez están más disponibles también en línea. Hay también muchos otros ejemplos en los que los legisladores de Estados miembros concretos han establecido una base jurídica para la publicación de datos personales de los individuos en internet o previa solicitud de acceso a los documentos. Entre estos figuran, por ejemplo[29]:

- gastos, salarios o declaraciones de conflicto de intereses de determinados funcionarios, o de beneficiarios de ayudas estatales (por ejemplo, subvenciones agrícolas);
- nombres de organizaciones o individuos que realizan donativos a partidos políticos;
- declaraciones fiscales de las personas físicas[30];
- resoluciones judiciales (con los nombres de las partes u otras personas a veces suprimidos o sustituidos por iniciales para reducir el riesgo de reidentificación);
- listas electorales;
- listas de audiencias judiciales que tendrán lugar en determinados días.

---

[28] Véase, no obstante, la sección 10.3 sobre «Condiciones de licencia para los conjuntos de datos anonimizados» y, en particular, la necesidad de establecer salvaguardias para contribuir a seguir garantizando que los individuos no serán reidentificados.

[29] Véanse también los ejemplos proporcionados en la sección V, al tratar el ámbito de la Directiva ISP.

[30] Véase, por ejemplo, la sentencia del Tribunal de Justicia de la Unión Europea de 16 de diciembre de 2008 en el asunto C-73/07 Tietosuojavaltuutettu contra Satakunnan Markkinapörssi Oy en Satamedia Oy.

En cada uno de estos casos, los organismos del sector público o los legisladores podrán considerar de manera proactiva si desean facilitar estos datos para su reutilización (por ejemplo, para mejorar servicios públicos tales como el acceso a los registros mercantiles o de la propiedad). Los posibles reutilizadores también podrán ponerse en contacto con los organismos del sector público para solicitar la reutilización de los datos. En otros casos, también es posible que los potenciales reutilizadores simplemente tomen los datos personales, que ya están disponibles en línea, y los utilicen sin ponerse en contacto necesariamente con el organismo del sector público que facilitó la información. En los tres casos, los reutilizadores tendrían que cumplir, por supuesto, con la legislación sobre protección de datos, ya que se trata de datos personales.

7.2. Diferencias entre los regímenes nacionales de acceso

Las obligaciones jurídicas para la puesta a disposición del público de determinados datos personales varían considerablemente entre los Estados miembros debido a la existencia de diferentes tradiciones culturales y jurídicas. En algunos Estados miembros existe una base jurídica que permite divulgar determinados datos personales, mientras que otros Estados miembros prohíben la divulgación de esos mismos datos en la misma situación. La Directiva ISP reconoce y deja claro que se basa en los regímenes de acceso vigentes en los Estados miembros y no modifica las normas nacionales de acceso a los documentos[31].

7.3. Necesidad de una evaluación de impacto sobre protección de datos y de garantías adecuadas

Como norma general, cuando se prevé facilitar datos personales para su reutilización, es estrictamente necesario seguir un enfoque prudente. El Grupo de trabajo del artículo 29, en particular, recomienda realizar una evaluación del impacto exhaustiva en materia de protección de datos antes de la publicación una serie de datos (o antes de adoptar una ley que requiera su publicación), que evalúe asimismo las posibilidades y el impacto potencial de la reutilización. En general, debe evitarse la apertura de los datos personales para su reutilización con una licencia abierta sin ninguna restricción técnica y jurídica en cuanto a la reutilización.

7.4. Importancia de un régimen de concesión de licencias

Además, el Grupo de trabajo del artículo 29 recomienda que se establezca un riguroso sistema de licencias, que también deberá ejecutarse adecuadamente para garantizar que los datos personales no se utilicen para fines incompatibles, por ejemplo, en el caso de mensajes comerciales no solicitados o de cualquier otra manera que los interesados puedan encontrar inesperada, inadecuada o nociva.

7.5. Importancia de una base jurídica sólida para la publicación y la reutilización

El Grupo de trabajo del artículo 29 reitera la importancia de establecer una base jurídica sólida para la publicación de datos personales, teniendo en cuenta las normas pertinentes sobre protección de datos, y en particular los principios de proporcionalidad, minimización de datos y limitación de la finalidad.

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 jurídica y la previsibilidad. En particular, por lo que respecta a las solicitudes de reutilización, será muy difícil

[31] Dicho esto, como se ha explicado en la sección 5.4, la legislación nacional debe cumplir el artículo 8 del CEDH y los artículos 7 y 8 de la Carta de la UE, según la interpretación de la jurisprudencia pertinente.

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.

Cualquier otra reutilización debe, en estos casos, contar con una base jurídica apropiada (por ejemplo, el consentimiento o un requisito legal) en virtud del artículo 7, letras a) a f), de la Directiva 95/46/CE y cumplir todos los demás principios de la protección de datos.

7.6. Limitación de la finalidad

Es difícil aplicar el principio de limitación de la finalidad de forma efectiva en caso de reutilización de la ISP. Por una parte, la propia idea y la fuerza impulsora de la innovación que se esconde tras el concepto de «datos abiertos» y reutilización de la ISP es que la información debe estar disponible para su reutilización para nuevos productos y servicios innovadores y, de este modo, para fines que no estén previamente definidos y no puedan preverse claramente. La Directiva ISP también exige que la concesión de licencias no sea innecesariamente restrictiva en cuanto a la reutilización.

Por otra parte, la limitación de la finalidad es un principio clave de la protección de datos y exige que los datos personales que se han recogido para un fin específico no se utilicen para otro propósito incompatible[32]. Este principio se aplica igualmente a los datos personales que están a disposición del público. El mero hecho de que los datos personales estén disponibles públicamente para una finalidad específica no significa que tales datos personales estén abiertos a la reutilización para cualquier otro fin.

Por ejemplo, los gastos de los altos cargos de las administraciones públicas se publican en internet en aras de la transparencia, pero su reutilización por cualquier persona para otros fines podrá no ser compatible.

Como se comenta más detalladamente en el Dictamen de 3/2013 del Grupo de trabajo del artículo 29 sobre limitación de la finalidad (véase la sección III.2.2 y el anexo 1), la evaluación de si un tratamiento ulterior de los datos personales es incompatible con los fines para los que dichos datos se han recopilado requiere una evaluación multifactorial. Se tendrá en cuenta, en particular:

a) la relación entre los fines para los que se recogieron los datos personales y los fines de su tratamiento ulterior;
b) el contexto en el que se recogieron los datos personales y las expectativas razonables de los interesados en cuanto a su uso ulterior;
c) la naturaleza de los datos personales y el impacto del tratamiento ulterior en los interesados;
d) las medidas de salvaguardia aplicadas por el responsable del tratamiento para garantizar el tratamiento leal y evitar que se produzcan repercusiones indebidas sobre los interesados.

Estos factores clave deben evaluarse cuando se tome la decisión de hacer públicos los datos personales, así como en cada caso en que vayan a reutilizarse los datos personales. A continuación figuran algunos ejemplos:

- Un organismo del sector público publica en un directorio información de contacto de sus funcionarios, en particular el nombre, cargo, dirección profesional y número de teléfono

[32] Los datos solo podrán utilizarse de forma incompatible con los fines especificados en el momento de su recogida de forma excepcional y con sujeción a estrictas garantías en virtud del artículo 13 de la Directiva 95/46/CE. Véase la sección III.3 del Dictamen 3/2013 del Grupo de trabajo del artículo 29 sobre limitación de la finalidad.

profesional. La finalidad evidente (aunque no se manifieste expresamente) del directorio es ayudar a los ciudadanos a determinar a quién dirigirse a la hora de realizar indagaciones y otras actividades oficiales. Un reutilizador desea recoger el contenido del directorio, combinarlo con las direcciones y números de teléfono privados de los empleados (cuando esta información esté a disposición del público, por ejemplo, en una guía telefónica), y facilitar las direcciones y números de teléfono tanto del domicilio como del trabajo en un mapa interactivo para mostrar donde viven y trabajan diferentes funcionarios. Esta combinación y reutilización de los datos debe considerarse incompatible con la finalidad inicial. Un funcionario cuya información de contacto de trabajo se publica para facilitar el contacto por parte de los ciudadanos, no esperaría razonablemente que esta información se relacione con otros datos que ha facilitado con una finalidad no relacionada con su trabajo.

- En algunos Estados miembros, en virtud de la legislación nacional, los anuncios de matrimonio son públicos y pueden ser consultados por cualquier persona. Esta publicación tiene por objeto advertir de la intención de una pareja de casarse y permitir a los interesados oponerse. No obstante, el hecho de que los datos personales contenidos en la publicación de los anuncios de matrimonio estén a disposición del público no permite a terceros utilizar esa información para enviar correo comercial a la pareja. Este uso adicional sería incompatible a la vista del objetivo de la publicación del anuncio de matrimonio, que es permitir la formulación de objeciones al matrimonio en virtud de la ley.

7.7. Fines comerciales frente a fines no comerciales

El Dictamen 7/2003 destaca las actividades comerciales como el principal incentivo para la reutilización de la ISP frente al acceso a la información, en que el objetivo de la legislación en materia de libertad de información es garantizar la transparencia, la apertura y la responsabilidad ante los ciudadanos.

El Dictamen 7/2003 también subraya que «[los ciudadanos] normalmente, utilizarán la información para sus propios fines, no comerciales». Esta declaración debe actualizarse a la luz de la experiencia adquirida desde entonces con la reutilización de la ISP. La experiencia con las iniciativas de datos abiertos ha demostrado que la reutilización de la ISP puede también contribuir perceptiblemente a aumentar la transparencia y la responsabilidad y puede conducir a un mejor uso de los servicios públicos. La distinción entre reutilización para fines comerciales o no comerciales no debería ser determinante al examinar la compatibilidad de una utilización ulterior de los datos personales. La evaluación de la compatibilidad no debe centrarse primordialmente en si el modelo económico de un posible reutilizador se basa o no en la obtención de beneficios.

Lo que debe evaluarse cuidadosamente es si los fines y la forma en que los datos se tratan ulteriormente son compatibles con los fines iniciales según los criterios mencionados en la sección 7.6. En el caso de reutilización de la ISP, esto conducirá inevitablemente a la consideración de una serie de situaciones de tratamiento, en lugar de una sola.

7.8. Proporcionalidad y otras preocupaciones

Otro principio fundamental previsto en la Directiva 95/46/CE es la proporcionalidad[33]. Existen numerosos métodos y modalidades distintos de publicar datos personales. Algunos pueden ser más intrusivos que otros y presentar mayores riesgos. Por tanto, algunos pueden considerarse proporcionados, mientras que otros no.

[33] Véase el artículo 6, apartado 1, letra c), de la Directiva 95/46/CE.

Al igual que sucede con la finalidad, preocupa la manera de controlar el tratamiento ulterior de los datos y garantizar el cumplimiento de otros principios de la normativa de protección de datos, en particular, pero no solo, la proporcionalidad. Una vez que los datos se han puesto a disposición del público, especialmente en internet, es muy difícil limitar efectivamente su uso y garantizar el cumplimiento de las normas sobre protección de datos.

Algunos retos a la hora de garantizar el cumplimiento de la legislación sobre protección de datos son los siguientes:

- cómo garantizar la actualización y la precisión de datos que están desconectados de su fuente originaria;
- cómo garantizar que el uso de los datos personales sigue limitándose a las funcionalidades previstas en la finalidad inicial de la publicación;
- cómo garantizar la oportuna supresión de datos si la publicación de los datos personales se ha previsto únicamente por un período de tiempo limitado[34];
- cómo ejercer los derechos de las personas en relación con los datos personales facilitados para su reutilización (incluido el derecho a solicitar la corrección, la actualización o la supresión).

7.9. Limitaciones legales o técnicas a la reutilización

A veces, la legislación o el diseño técnico de los sistemas limitan algunas operaciones específicas de tratamiento o establecen otras salvaguardias que limitan el uso de los registros públicos (por ejemplo, limitando la posibilidad de descargar todo el contenido del registro o limitando las búsquedas, por ejemplo, basadas en el nombre y apellido de un individuo). En este caso, la reutilización debería permitirse en principio únicamente de conformidad con estas condiciones y limitaciones específicas.

En este contexto, es importante analizar atentamente qué medidas (tanto legales como técnicas) podrían establecerse a fin de contribuir a garantizar que se abordarán las preocupaciones sobre protección de datos, en particular las señaladas en la sección 7.8. Es especialmente importante considerar la forma en que los reutilizadores tendrán acceso a los datos, por ejemplo a través de una función de descarga a granel o a través de una interfaz personalizada con capacidades de acceso limitadas con sujeción a determinadas condiciones. A este respecto, son cruciales los controles de seguridad suplementarios que se aplicarán, como, por ejemplo, un sistema de verificación con imagen distorsionada «captcha»[35] para evitar el acceso automatizado y minimizar el riesgo de recogida de toda una base de datos. La utilización de medidas técnicas específicas puede contribuir a reducir el uso indebido de datos personales y los efectos negativos en los interesados que de otro modo podrían darse mediante el acceso ilimitado e incondicional de los reutilizadores a la totalidad de los conjuntos de datos.

Es importante tener en cuenta que, en muchos casos, puede ser necesario garantizar que los reutilizadores solo puedan realizar consultas específicas mediante tecnologías que impidan la descarga a granel de registros de datos, por ejemplo mediante interfaces de programas de aplicación

[34] Véase, por ejemplo, el asunto ante el Tribunal de Justicia Europeo Volker und Markus Schecke GbR / Land Hessen (asuntos acumulados C 92/09 y C 93/09), apartado 31: «resulta imposible retirar los datos de Internet tras la expiración del plazo de dos años establecido en el artículo 3, apartado 3, del Reglamento nº 259/2008».

[35] Un CAPTCHA (Prueba de Turing pública y automática para diferenciar máquinas y humanos) es un sistema de respuesta diseñado para distinguir a los humanos de los programas automáticos. Un CAPTCHA distingue entre un humano y un ordenador encargando una tarea que resulta sencilla para la mayoría de los humanos pero que es más difícil que la realicen programas de ordenador.

(«API») a medida. Ello puede contribuir a garantizar la proporcionalidad del uso y reducir los riesgos de utilización abusiva de bases de datos enteras. Además, estas interfaces a medida también pueden ayudar a garantizar que los datos estén siempre actualizados, y además, que los datos no estén disponibles a través de la API una vez se haya adoptado una decisión a tal efecto por el organismo del sector público de que se trate. Por otra parte, podrán limitar las formas en que un reutilizador puede reutilizar los datos.

7.10. Exactitud, actualización y supresión

Otra cuestión específica es lo que ocurre si los datos personales se publican o se ponen a disposición del público de alguna manera solo durante un período de tiempo limitado. El artículo 6, apartado 1, letra e), de la Directiva 95/46/CE establece que los datos personales deberán ser conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente. El considerando 18 de la Directiva ISP también establece que «cuando la autoridad competente decida no seguir permitiendo la reutilización de determinados documentos, o dejar de actualizarlos, debe hacer públicas estas decisiones en el plazo más breve y, si ello es posible, por vía electrónica».

No obstante, resulta difícil y a veces imposible cerciorarse de que los datos se supriman o eliminen una vez se hayan publicado y facilitado para su reutilización.

A este respecto, puede aportarse una cierta solución (aunque en modo alguno completa) si los datos no se facilitan en formato descargable, sino únicamente a través de una API específica y sujeta a determinadas restricciones y medidas de seguridad, como se ha indicado anteriormente.

VIII. Datos de investigación

En este caso es importante establecer una distinción entre la publicación de datos anonimizados por una parte (véase la sección VI) y al acceso limitado, por otra. El programa de apertura de datos se basa claramente en la disponibilidad pública de estos. Sin embargo, gran parte de las investigaciones (en general, la investigación científica, tanto para fines comerciales como no comerciales, pero también otro tipo de investigaciones) derivan de la divulgación de datos dentro de una comunidad cerrada, es decir, en la que un número limitado de investigadores o instituciones tienen acceso a los datos y en la que es posible restringir la divulgación o utilización ulterior de los datos y puede garantizarse la seguridad de estos.

El acceso limitado es especialmente importante para el tratamiento de datos personales (a menudo en forma de pseudónimos[36]) derivados de datos sensibles, o cuando exista un riesgo elevado de reidentificación. Puede haber riesgos asociados a la divulgación con acceso limitado, pero son menores y pueden atenuarse cuando los datos se divulgan en una comunidad cerrada que trabaja con normas establecidas.

Un problema que a menudo padecen las personas que utilizan datos con fines de investigación es que, por una parte, desean que los datos sean ricos, granulares, y suficientemente utilizables para sus fines; y por otra, desean garantizar que no pueda realizarse la reidentificación de las personas. Por un lado, los datos pseudonimizados individualizados a nivel personal (por ejemplo, sencillamente

[36] Véase de nuevo el Dictamen 4/2007 sobre el concepto de datos personales, adoptado el 20.6.2007 (WP 136), especialmente las pp. 12-21 («datos relativos a seudónimos», «datos cifrados» y «datos anónimos» en las pp. 18-21). La cuestión de la información «relativa a» un individuo se trata en las pp. 9-12. También cabe señalar, como se indica en la página 3, que el Grupo de trabajo del artículo 29 está trabajando actualmente en proporcionar mayor orientación sobre técnicas de anonimización.

cifrados) pueden ser muy valiosos para los investigadores por su precisión y porque los datos pseudonimizados de diversas fuentes pueden cotejarse de forma relativamente fácil. Sin embargo, esto también significa que existe un alto riesgo de reidentificación: la posibilidad de relacionar varios conjuntos de datos (pseudonimizados o no) con la misma persona puede ser un paso previo a la identificación, o puede permitir una identificación directa.

Por tanto, se precisa una evaluación minuciosa y precauciones adicionales antes de publicar conjuntos de datos pseudonimizados o facilitarlos para su reutilización. En general, cuanto más detallados, relacionables e individualizados son los datos, más limitado y controlado debería ser el acceso a los mismos. Cuanto más agregados y menos relacionables sean, más probable será que puedan publicarse y facilitarse para su reutilización sin riesgos significativos.

Este es un ámbito complejo y en constante evolución y no sería procedente excluir categóricamente la publicación y la reutilización de todos los conjuntos de datos que no alcanzan el elevado umbral de «anonimización» descrito en la sección VI. Dicho esto, y si bien siempre se precisa un análisis caso por caso y una evaluación cuidadosa, el Grupo de trabajo del artículo 29 considera que en general, la liberación de acuerdo con las disposiciones de la Directiva ISP de conjuntos de datos individualizados, o de otros conjuntos de datos que presentan un riesgo significativo de reidentificación, a menudo no será adecuada.

Además, es importante poner de relieve que en caso de que algunos de estos grupos de datos se publiquen y pongan a disposición, tras una minuciosa evaluación de los riesgos y los beneficios, la divulgación y cualquier otra reutilización ulterior deben realizarse respetando plenamente la legislación sobre protección de datos (véase la sección VII). Esto se debe a que estos datos, a pesar de la adopción de medidas (a veces muy importantes) adoptadas para reducir los riesgos de reidentificación, no obstante siguen considerándose datos personales.

IX. Archivos históricos

Los archivos históricos y los museos también tienen características específicas que requieren garantías concretas. En muchos casos, y en función de factores como la edad y la sensibilidad de los datos y el contexto de la recogida, otras opciones (como permitir el acceso restringido con sujeción solamente a las obligaciones de confidencialidad) pueden ser más adecuadas que digitalizar y facilitar los datos para su reutilización a través de internet, sin restricciones.

Con respecto a los archivos, también es importante hacer hincapié en que, aunque la sensibilidad de los datos, en general, se reducirá con el tiempo, la liberación inadecuada de registros con una antigüedad de muchas décadas puede tener un efecto muy perjudicial en las personas directamente afectadas y también en otras personas, como los miembros de sus familias o sus descendientes. Esto es especialmente cierto respecto de los datos muy sensibles. Por ejemplo, la liberación de registros de antecedentes penales estigmatizaría a una persona y obstaculizaría su reinserción. Asimismo, la información de que una persona fallecida ha sido un agente secreto o un colaborador de un régimen represivo, un pedófilo, un delincuente, un enfermo mental estigmatizado, o ha padecido una enfermedad hereditaria, puede también tener consecuencias negativas en la familia (por ejemplo, el cónyuge superviviente, los hijos, u otros descendientes) de la persona fallecida. Las muestras de ADN de los restos mortales de las personas físicas, que a veces se conservan en los archivos de los hospitales públicos, también podrían requerir protección por razones similares. Por tanto, este tipo de información, incluso en el caso de que esté relacionada con personas fallecidas, podrá exigir protección con arreglo a la legislación sobre protección de datos u otras leyes de protección de los derechos fundamentales, según el caso.

Los Estados miembros tienen a menudo leyes específicas que rigen el acceso a los archivos nacionales, los archivos de los períodos históricos recientes de especial interés (tales como archivos que atestigüen la colaboración con regímenes opresores), y los expedientes del poder judicial[37]. Estas leyes requieren a menudo medidas de seguridad apropiadas y restricciones de acceso y otras salvaguardias destinadas a equilibrar los intereses en juego y a garantizar la accesibilidad de determinados datos personales con fines de investigación histórica, transparencia e investigaciones periodísticas, garantizando al mismo tiempo que la revelación de información, en su caso, sea limitada de modo que no perjudique a la vida privada y familiar y a la dignidad de las partes interesadas.

Con respecto a la «limitación de la finalidad», cabe señalar que los archivos históricos normalmente almacenan información para fines de investigación histórica. Estos fines son diferentes de los fines iniciales para los que fueron recogidos. El material que acabará en las colecciones de archivos se creó inicialmente para determinados fines administrativos por diferentes organismos del sector público. Normalmente, tras un determinado período de tiempo, cuando el documento ya no es necesario para los fines administrativos originales, se realiza un proceso de selección y los documentos que se considere que pueden tener valor «histórico» se transfieren a los archivos históricos. La cuestión que se plantea aquí es para qué fines deberían estar disponibles para su reutilización los datos personales almacenados en los archivos. En este contexto, es importante realizar una evaluación detallada, considerando el valor potencial de la divulgación del material de archivo para su reutilización, pero también la posible incidencia en los derechos, libertades y dignidad de las personas interesadas.

De forma general, puede concluirse que, aunque la digitalización de determinados registros que contengan datos personales y su facilitación para la reutilización puedan resultar adecuadas en algunas situaciones, y algunos datos puedan también divulgarse de forma anonimizada, en otros casos son de primordial importancia la limitación de la divulgación y la reutilización de los datos personales y la aplicación de medidas de seguridad adecuadas para proteger dichos datos. Una evaluación del impacto sobre la protección de datos minuciosa debe garantizar que ninguna colección de archivo se facilite para su reutilización a menos que pueda excluirse cualquier efecto potencial negativo sobre las personas interesadas o que los posibles riesgos se reduzcan al mínimo aceptable. El sector de los archivos debería prever asimismo la elaboración de códigos de conducta o la modificación de los códigos vigentes para explicar las buenas prácticas.

X. Concesión de licencias para la reutilización de datos personales

10.1. Disposiciones pertinentes de la Directiva ISP

El considerando 15 de la Directiva ISP establece que «garantizar que las condiciones de reutilización de los documentos del sector público sean claras y estén a disposición del público constituye una condición previa para el desarrollo de un mercado de la información que abarque la totalidad de la Comunidad. Por consiguiente, debe informarse claramente a los reutilizadores potenciales de todas las condiciones aplicables a la reutilización de documentos. Los Estados miembros deben alentar la creación de índices accesibles en línea, cuando sea oportuno, de los documentos disponibles para fomentar y facilitar las solicitudes de reutilización».

[37] Otros ejemplos pueden ser los archivos de los registros civiles, que en algunos Estados miembros contienen, entre otros, las causas de la muerte, la modificación del sexo, el nombre del cónyuge (de lo que puede deducirse la orientación sexual), o el hecho de que un individuo haya sido adoptado. El acceso a estos archivos también está sujeto a condiciones específicas.

El considerando 26 de la Directiva ISP modificada establece, además, que «en relación con cualquier tipo de reutilización de un documento, es conveniente que los organismos del sector público puedan, en su caso mediante licencia, imponer condiciones ... » y que «cuando proceda, los Estados miembros deben fomentar el uso de formatos abiertos y legibles por máquina».

Asimismo, el artículo 8, apartado 1, establece que «los organismos del sector público podrán autorizar la reutilización de documentos sin condiciones o bien podrán imponer condiciones, en su caso mediante una licencia. Estas condiciones no restringirán sin necesidad las posibilidades de reutilización y no se usarán para restringir la competencia».

10.2. Concesión de licencias y protección de datos

Las licencias son una parte fundamental del régimen ISP. También pueden afectar a la forma en que se tratan los datos personales y deberían figurar entre las salvaguardias aplicables a la hora de facilitar los datos personales (o los datos anonimizados derivados de los datos personales) para su reutilización. Las licencias no eliminan la necesidad de cumplir con la legislación sobre protección de datos, pero una cláusula de protección de datos en las condiciones establecidas en las licencias ayudaría a garantizar el cumplimiento de la legislación sobre protección de datos al añadir una «fuerza ejecutiva». Dicha cláusula podría también contribuir a aumentar la sensibilización recordando a los reutilizadores sus obligaciones como responsables del tratamiento de los datos.

En relación con el contenido de las licencias, cabe distinguir dos situaciones diferentes.

10.3. Condiciones de licencia para conjuntos de datos anonimizados

En primer lugar, en cuanto a los datos anonimizados (es decir, conjuntos de datos que ya no contienen datos personales), las condiciones para la concesión de licencias deben:

- reiterar la anonimización de los conjuntos de datos;
- prohibir a los titulares de licencias reidentificar a las personas[38];
- prohibir a los titulares de licencias utilizar los datos para tomar cualquier medida o decisión respecto a las personas de que se trate; y
- también debe incluirse la obligación del titular de una licencia de notificar a la entidad que expide las licencias en caso de que detecte que las personas pueden ser reidentificadas o lo han sido ya.

Como alternativa a una condición de licencia, puede incluirse un mensaje de advertencia para los reutilizadores, de forma ostensible, en el portal de datos abiertos. No obstante, la adopción de condiciones para la concesión de licencias debe promoverse porque tendría la ventaja añadida de tener fuerza ejecutoria contractual.

Retirada de conjuntos de datos comprometidos

La posibilidad de alertar al licenciante de que se ha producido una reidentificación o de que puede producirse debe estar abierta a todos los demás usuarios de la web, incluidos los propios interesados.

[38] Cabe aplicar excepciones limitadas, por ejemplo, en casos de pruebas de reidentificación de buena fe. Incluso en tales casos, los resultados de las pruebas deben comunicarse al responsable del tratamiento y al organismo del sector público en cuestión, y los datos reidentificados no deben publicarse ni divulgarse de ninguna otra manera.

Cuando el licenciante descubra un mayor riesgo de reidentificación, debe preverse en la licencia un procedimiento por el que el licenciante pueda «retirar» el conjunto de datos «comprometido». En otras palabras, la cláusula de protección de datos debería dar al licenciante el derecho de suspender o poner fin a la accesibilidad de los datos (por ejemplo, el derecho a desconectar la API o eliminar el archivo de la plataforma). El licenciante debería hacer todos los esfuerzos razonables para exigir a todos los reutilizadores que supriman la totalidad o una parte de los conjuntos de datos comprometidos (reidentificables). Esto debería incluir advertencias destacadas en sitios web como portales de datos abiertos y foros, listas de correo electrónico y medios sociales a los que accedan los grupos o individuos que puedan reutilizar los datos. La exigencia de registro puede ser el medio más eficaz para retirar los conjuntos de datos, pero esto no debe fomentarse si requiere la recopilación de nuevos datos personales de los reutilizadores, y tendría un efecto disuasorio general para el uso de los sitios web de IPS y otros servicios.

10.4. Condiciones de licencia para datos personales

Cuando los datos personales son objeto de una licencia, es necesario establecer los límites de la utilización de estos datos. En este caso, la principal preocupación es garantizar que toda reutilización se limite a lo que pueda ser «compatible con los fines para los que los datos hayan sido inicialmente recogidos»[39]. Para lograrlo, las condiciones de la licencia deben al menos indicar claramente para qué fines se publicaron por primera vez los datos y dar una indicación de lo que podría y lo que no podría considerarse una utilización compatible de los datos personales.

Hay que señalar, no obstante, que estas condiciones «no restringirán sin necesidad las posibilidades de reutilización» (artículo 8, apartado 1, de la Directiva ISP modificada). Esto puede a menudo significar que las condiciones genéricas de las licencias tipo abiertas no son adecuadas y que puede ser preciso desarrollar licencias específicas para determinados datos personales, o que pueden utilizarse plantillas, que podrían adaptarse.

En la actualidad, algunas licencias tipo abiertas (como la licencia gubernamental abierta del Reino Unido) excluyen los datos personales – que, de acuerdo con las condiciones establecidas, no se conceden en ningún caso.

10.5. Imposición de sanciones en caso de reidentificación o de uso incompatible

Una vez publicados los datos con arreglo a una licencia, como una licencia abierta del gobierno, puede ser difícil protegerlos de una ulterior utilización o divulgación incompatibles o mantenerlos seguros. El control de la reutilización y la sanción de cualquier tipo de violación, ya sea en forma de reidentificación de los interesados o su utilización ulterior para un propósito incompatible con el descrito por el licenciante, es muy importante en este contexto.

Si bien el Grupo de trabajo del artículo 29 reitera la importancia del papel que deben desempeñar los organismos del sector público, también resalta que, cuando un reutilizador recoge datos personales mediante un proceso de reidentificación, lo más probable es que se considere que está tratando los datos personales ilegalmente y podría ser objeto de sanciones por las autoridades responsables de la protección de datos. Esto incluye severas multas en el marco de la propuesta de Reglamento de protección de datos.

[39] Véase de nuevo el Dictamen 3/2013 del Grupo de trabajo del artículo 29 sobre limitación de la finalidad.

XI. Conclusiones

En conclusión, el Grupo de trabajo del artículo 29 reitera que la reutilización de la ISP puede aportar beneficios que conduzcan a una mayor transparencia y una reutilización innovadora de la información del sector público. No obstante, esta mayor accesibilidad de la información resultante no está exenta de riesgos. Con el fin de garantizar la protección de la intimidad y de los datos personales, es preciso seguir un enfoque equilibrado y la legislación sobre protección de datos deberá contribuir a orientar el proceso de selección de los datos personales que pueden o no pueden facilitarse para su reutilización y las medidas que deben tomarse para proteger los datos personales.

Independientemente del «principio de reutilización» formulado en la modificación ISP, la reutilización para fines comerciales o no comerciales de conformidad con las disposiciones de la Directiva ISP no siempre es adecuada en los casos en que la ISP que vaya a ser reutilizada contenga datos personales. En vez de datos personales, son a menudo datos estadísticos derivados de datos personales los que se facilitan y deben facilitarse para su reutilización.

No obstante, en algunas situaciones, puede también ser posible que los datos personales puedan considerarse disponibles para su reutilización según los términos de la Directiva ISP, en caso necesario, con sujeción a medidas legales, técnicas o de organización adicionales para proteger a los interesados. Para estos casos, el Grupo de trabajo del artículo 29 reitera la importancia de establecer una base jurídica sólida para la publicación de datos personales, teniendo en cuenta las normas pertinentes de protección de datos, incluidos los principios de proporcionalidad, de minimización de datos y de limitación de la finalidad. En este contexto, es también importante subrayar de nuevo que toda información relativa a una persona física identificada o identificable, ya esté a disposición del público o no, constituye datos personales. Por tanto, el acceso y la reutilización de datos personales que se hayan puesto a disposición del público siguen sujetos a la legislación sobre protección de datos aplicable.

A la luz de estas consideraciones, el Grupo de Trabajo del Artículo 29 recomienda lo siguiente:

- el hecho de que algunas ISP puedan contener datos personales debe tenerse en cuenta cuanto antes cuando se plantee poner la ISP a disposición del público, con arreglo a los principios de «protección de datos desde el diseño y por defecto»;
- teniendo esto en cuenta, el organismo del sector público en cuestión (o el legislador, según el caso) deberá realizar una evaluación de impacto de la protección de datos antes de facilitar para su reutilización cualquier ISP que contenga datos personales (o antes de adoptar una ley que permita la publicación de datos personales, haciéndolos por tanto potencialmente disponibles para su reutilización); también debería realizarse una evaluación de impacto de la protección de datos en situaciones en las que se faciliten para su reutilización grupos de datos anonimizados derivados de datos personales;
- cuando se anonimicen conjuntos de datos, es esencial evaluar el riesgo de reidentificación, y es una buena práctica realizar una prueba de reidentificación;
- el resultado de la evaluación podría ayudar a identificar salvaguardias adecuadas para reducir al mínimo los riesgos, en particular, y sin limitación alguna, medidas técnicas, jurídicas y organizativas tales como condiciones adecuadas para la concesión de licencias y medidas técnicas para evitar la descarga de datos a granel, y técnicas de anonimización adecuadas; también podrá decidirse no publicar los datos ni facilitarlos para su reutilización;
- las condiciones de la licencia para reutilizar la ISP deberán incluir una cláusula de protección de datos, cuando los datos personales sean objeto de tratamiento, incluso en situaciones en

las que grupos de datos anonimizados derivados de datos personales se pongan a disposición para su reutilización;

- cuando la evaluación de impacto llegue a la conclusión de que una licencia abierta no es suficiente para hacer frente a los riesgos de protección de datos, los organismos del sector público no deberán facilitar datos personales en el marco de la Directiva ISP. (Sin embargo, el organismo del sector público podrá utilizar su discrecionalidad para considerar la reutilización al margen de los términos y el alcance de la Directiva ISP y podrá exigir asimismo que los solicitantes demuestren que los riesgos para la protección de los datos personales se abordan de forma adecuada y que el solicitante tratará los datos de conformidad con la legislación aplicable sobre protección de datos);
- en su caso, los organismos del sector público deberán garantizar que los datos personales sean anonimizados y que las condiciones para la concesión de licencias prohíban específicamente la reidentificación de las personas y la reutilización de los datos personales para fines que puedan afectar a los interesados;
- por último, los Estados miembros deberán considerar además la creación y el apoyo a redes de conocimientos y centros de excelencia, permitiendo así la puesta en común de buenas prácticas relativas a la anonimización y los datos abiertos.

Hecho en Bruselas, el 5 de junio de 2013

Por el Grupo de trabajo
El Presidente
Jacob KOHNSTAMM