01248/07/ES
WP 136

Dictamen 4/2007 sobre el concepto de datos personales

Adoptado el 20 de junio

EL GRUPO 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[1],

Visto el artículo 29 y el artículo 30, apartado 1, letra a), y apartado 3, de dicha Directiva, y el artículo 15, apartado 3, de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002,

Visto el artículo 255 del Tratado CE y el Reglamento (CE) n° 1049/2001 del Parlamento Europeo y del Consejo, de 30 de mayo de 2001, relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión,

Visto su Reglamento interno,

HA ADOPTADO EL PRESENTE DICTAMEN:

[1] DO L 281 de 23.11.1995, p. 31, disponible en: http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm.

I. INTRODUCCIÓN.....3

II. CONSIDERACIONES GENERALES Y CUESTIONES POLÍTICAS.....4

III. ANÁLISIS DE LA DEFINICIÓN DE «DATOS PERSONALES» SEGÚN LA DIRECTIVA DE PROTECCIÓN DE DATOS.....6

1. PRIMER COMPONENTE: «TODA INFORMACIÓN».....6

2. SEGUNDO COMPONENTE: «SOBRE».....9

3. TERCER COMPONENTE: [PERSONA FÍSICA] «IDENTIFICADA O IDENTIFICABLE».....13

4. CUARTO COMPONENTE: «PERSONA FÍSICA».....24

IV. ¿QUÉ SUCEDE SI LOS DATOS NO ENCAJAN DENTRO DE LA DEFINICIÓN?.....26

V. CONCLUSIONES.....27

I. INTRODUCCIÓN

El Grupo de trabajo es consciente de la necesidad de llevar a cabo un profundo análisis del concepto de datos personales. La información de que se dispone sobre la práctica actual en los Estados miembros de la UE sugiere que existe una cierta incertidumbre y una cierta diversidad entre los Estados miembros en relación con aspectos importantes de este concepto que pueden afectar al correcto funcionamiento del actual marco de protección de datos en diversos ámbitos. El resultado de este análisis de un elemento central para la aplicación e interpretación de las normas sobre protección de datos tendrá sin duda un profundo impacto en varios temas importantes y, en especial, en relación con asuntos tales como la gestión de la identidad en el contexto de los sistemas electrónicos al servicio de la administración pública y de la sanidad (e-Gobierno y sanidad en línea), así como en el de la RFID (identificación por radiofrecuencia).

El objetivo del presente Dictamen del Grupo de trabajo es alcanzar un acuerdo sobre el concepto de datos personales, los casos en que debe aplicarse la legislación nacional sobre protección de datos y la manera en que ésta debe aplicarse. Alcanzar una definición común del concepto de datos personales equivale a definir lo que entra o queda fuera del ámbito de aplicación de las normas sobre protección de datos. Un corolario de este trabajo es prestar orientación sobre la manera en que las normas nacionales sobre protección de datos deben aplicarse a determinadas categorías de situaciones que se dan en Europa y contribuir, por lo tanto, a la aplicación uniforme de tales normas, que es una de las tareas fundamentales del Grupo de trabajo del artículo 29.

Este documento utiliza ejemplos extraídos de la práctica nacional de las autoridades de protección de datos europeas para apoyar e ilustrar el análisis. La mayor parte de los ejemplos sólo se han recogido para su uso en este contexto.

II. CONSIDERACIONES GENERALES Y CUESTIONES POLÍTICAS

La Directiva maneja un concepto lato de datos personales

La definición de datos personales contenida en la Directiva 95/46/CE (en adelante «la Directiva sobre protección de datos» o «la Directiva») reza así:

«"datos personales": 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».

Resulta necesario señalar que esta definición refleja la intención del legislador europeo de mantener un concepto amplio de «datos personales» a lo largo de todo el proceso legislativo. En la propuesta original de la Comisión se explicaba que *«como en el Convenio 108, se adopta una definición amplia para abarcar toda información que pueda vincularse a una persona»*[2]. La propuesta modificada de la Comisión señalaba que *«la propuesta modificada recoge el deseo del Parlamento de que la definición de "datos personales" sea tan amplia como sea posible con el fin de incluir toda información referente a una persona identificable»*[3], un deseo que también el Consejo tuvo en cuenta en la posición común[4].

El objetivo de las normas incluidas en la Directiva es proteger a las personas

El artículo 1 de la Directiva 95/46/CE y el artículo 1 de la Directiva 2002/58/CE no dejan lugar a dudas sobre el principal objetivo de las normas en ellas incluidas: proteger las libertades y los derechos fundamentales de las personas físicas y, en particular, su derecho a la intimidad, en lo que respecta al tratamiento de los datos personales. Éste es un elemento muy importante que debe tenerse en cuenta al interpretar y aplicar las normas contenidas en ambos instrumentos. Puede ser fundamental a la hora de determinar la manera de aplicar las disposiciones de la Directiva a determinadas situaciones en las que los derechos individuales no están en peligro y puede jugar en contra de cualquier interpretación de esas mismas normas que prive a las personas físicas de la protección de sus derechos individuales.

El ámbito de aplicación de la Directiva excluye varias actividades y la flexibilidad impregna el texto con el fin de proporcionar una respuesta legal apropiada a las circunstancias imperantes en cada caso

A pesar de la amplitud de los conceptos de «datos personales» y de «tratamiento» utilizados en la Directiva, el simple hecho de que pueda considerarse que una determinada situación implica el «tratamiento de datos personales» con arreglo a la

---

2 COM (90) 314 final de 13.9.1990, p. 19 (comentario sobre el artículo 2).
3 COM (92) 422 final de 28.10.1992, p. 10 (comentario sobre el artículo 2).
4 Posición Común (CE) nº 1/95 adoptada por el Consejo el 20 de febrero de 1995, DO C 93 de 13.4.1995, p.25.

definición no determina por sí solo que esa situación esté cubierta por las normas de la Directiva, en especial de conformidad con su artículo 3. Aparte de las exenciones que tienen su origen en el ámbito de aplicación del Derecho comunitario, las exenciones previstas en el artículo 3 de la Directiva tienen en cuenta la forma técnica del tratamiento (en forma manual no estructurada) y el fin con el que se utilizan (para las actividades exclusivamente personales o domésticas efectuadas por una persona física). Pero, incluso en el supuesto de que el tratamiento de datos personales entre en el ámbito de la Directiva, puede que no todas sus normas sean aplicables al caso concreto. Varias disposiciones de la Directiva tienen un grado de flexibilidad considerable, con el fin de lograr un equilibrio adecuado entre la protección de los derechos del interesado, por un lado, y los posibles intereses legítimos de los responsables del tratamiento de datos, las terceras personas y el interés público, por otro. Algunos ejemplos de tales disposiciones se recogen en el artículo 6 (período de conservación de los datos en función de la necesidad de los mismos), artículo 7, letra f) (equilibrio de intereses para justificar el tratamiento), artículo 10, letra c), último guión, y artículo 11, apartado 1, letra c) (información necesaria para garantizar un tratamiento leal de los datos), o en el artículo 18 (exenciones de la obligación de notificación), por no mencionar más que algunos casos.

El alcance de las normas de protección de datos no debe llevarse hasta sus extremos

Un resultado no deseado sería el de terminar aplicando las normas de protección de datos a situaciones que, en principio, no deberían estar cubiertas por estas normas; y para las que no fueron concebidas por el legislador. Las exenciones sustanciales previstas en el artículo 3 mencionado anteriormente y las aclaraciones de los considerandos 26 y 27 de la Directiva muestran cómo quería el legislador que se aplicara la protección de datos.

Una de las limitaciones se refiere a la manera de tratar los datos. Es útil recordar que la adopción de las primeras leyes de protección de datos, en los años setenta, tuvo su razón de ser en el hecho de que una nueva tecnología, el tratamiento electrónico de datos, permitía un acceso más fácil y más amplio a los datos personales que las formas tradicionales utilizadas hasta entonces. En consecuencia, de acuerdo con la Directiva, la protección de datos aspira a proteger esas técnicas de tratamiento que generalmente encierran un mayor riesgo de que se pueda «*acceder fácilmente a los datos personales*» (considerando 27). El tratamiento no automatizado de datos personales sólo entra en el ámbito de la Directiva cuando los datos están contenidos o destinados a ser incluidos en un fichero (artículo 3).

Otra limitación de índole general que pesa sobre la aplicación de la protección de datos prevista por la Directiva es la del tratamiento de datos en circunstancias, en las que los medios para identificar al interesado no «*puedan ser razonablemente utilizados*» (considerando 26), una cuestión que se analizará más adelante.

Pero también debe evitarse una limitación indebida de la interpretación del concepto de datos personales.

En aquellos casos en que, a primera vista, una aplicación mecánica de una determinada disposición de la Directiva provoque una carga excesiva o incluso consecuencias absurdas, deberá comprobarse previamente: 1) si la situación entra en el ámbito de aplicación de la Directiva, en particular con arreglo a su artículo 3; y 2) cuando así sea, si la propia Directiva, o la legislación nacional adoptada de conformidad con ella, no

admite exenciones o simplificaciones en situaciones particulares con el fin de lograr una respuesta legal apropiada, asegurando al mismo tiempo la protección de los derechos de la persona y los intereses en juego. La mejor opción es no restringir indebidamente la interpretación de la definición de datos personales, sino tener en cuenta que existe una considerable flexibilidad en la aplicación de las normas a los datos.

Las autoridades nacionales encargadas de supervisar la protección de datos tienen un rol esencial a este respecto dentro de su función de supervisión de la aplicación de la legislación sobre protección de datos, que conlleva interpretar las disposiciones legales y proporcionar orientación concreta a los responsables y los interesados. Esas autoridades deberían aprobar una definición lo suficientemente amplia para anticiparse a las posibles evoluciones y cubrir todas las «zonas grises» existentes en su ámbito de aplicación, haciendo al mismo tiempo uso legítimo de la flexibilidad que caracteriza a la Directiva. De hecho, el texto de la Directiva invita a elaborar una política que combine una interpretación lata del concepto de datos personales y un equilibrio apropiado en la aplicación de sus normas.

III. ANÁLISIS DE LA DEFINICIÓN DE «DATOS PERSONALES» SEGÚN LA DIRECTIVA DE PROTECCIÓN DE DATOS

La definición de la Directiva consta de cuatro componentes principales, que se analizarán por separado a los efectos del presente documento. Esos cuatro componentes son:

- «toda información»
- «sobre»
- «identificada o identificable»
- «persona física»

Estos cuatro componentes están estrechamente ligados y se complementan recíprocamente. Sin embargo, en aras de la metodología seguida en este documento, cada uno de ellos se analiza por separado.

1. PRIMER COMPONENTE: «TODA INFORMACIÓN»

La expresión «toda información» utilizada en la Directiva indica claramente la voluntad del legislador de dar un sentido amplio al concepto «datos personales». Esta redacción exige una interpretación amplia.

Desde el punto de vista de la naturaleza de la información, el concepto de datos personales incluye todo tipo de afirmaciones sobre una persona. Por consiguiente, abarca información «objetiva» como, por ejemplo, la presencia de determinada sustancia en su sangre, pero también informaciones, opiniones o evaluaciones «subjetivas». Esta última clase de afirmaciones constituye una parte considerable del caudal de datos personales tratados en sectores como el de la banca, para evaluar la fiabilidad de los prestatarios («Fulano es un prestatario fiable»), el asegurador («no se espera que Fulano muera pronto») o el laboral («Fulano es un buen trabajador y merece un ascenso»).

Para que esas informaciones se consideren «datos personales», no es necesario que sean verídicas o estén probadas. De hecho, las normas de protección de datos prevén la posibilidad de que la información sea incorrecta y confieren al interesado el derecho de acceder a esa información y de refutarla a través de los medios apropiados[5].

Desde el punto de vista del contenido de la información, el concepto de datos personales incluye todos aquellos datos que proporcionan información cualquiera que sea la clase de ésta. Por supuesto esto incluye la información personal considerada «datos sensibles» en el artículo 8 de la Directiva a causa de su naturaleza particularmente delicada, pero también otras categorías más generales de información. El término «datos personales» comprende la información relativa a la vida privada y familiar del individuo *stricto sensu*, pero también la información sobre cualquier tipo de activad desarrollada por una persona, como la referida a sus relaciones laborales o a su actividad económica o social. El concepto de «datos personales» abarca, por lo tanto, información sobre las personas, con independencia de su posición o capacidad (como consumidor, paciente, trabajador por cuenta ajena, cliente, etc.).

Ejemplo nº 1: Hábitos y prácticas profesionales

La información sobre la prescripción de un medicamento (por ejemplo, el número de identificación del medicamento, su nombre, su concentración, el fabricante, el precio de venta, si se trata de una nueva prescripción o de un fármaco que ya se está tomando, los motivos para su uso, las razones para no suministrar un medicamento genérico, el nombre y apellidos de la persona que lo prescribe, número de teléfono, etc.), tanto si se trata de una receta individual como de un tratamiento pautado, puede considerarse como «datos personales» sobre el médico que lo prescribe, aunque el paciente sea anónimo. Así pues, proporcionar información sobre recetas expedidas por médicos identificados o identificables a las industrias farmacéuticas constituye una comunicación de datos personales a terceros con arreglo a la Directiva.

Esta interpretación se basa en la propia redacción de la Directiva. Por una parte, hay que considerar que el concepto de vida privada y familiar es sumamente amplio, tal como el Tribunal Europeo de Derechos Humanos dejó claro[6]. Por otra, las normas sobre protección de datos personales van más allá de la protección del amplio concepto del derecho al respeto de la vida privada y familiar. Cabe señalar que, en su artículo 8, la Carta de los Derechos Fundamentales de la Unión Europea consagra la protección de los datos de carácter personal como un derecho autónomo, separado y diferente del derecho al respeto de la vida privada, mencionado en su artículo 7, y lo mismo sucede en algunos Estados miembros. Esto se ajusta a los términos del artículo 1, apartado 1, de la Directiva, dirigido a la protección de «*las libertades y los derechos fundamentales de las personas físicas y, en particular* [pero no exclusivamente] *del derecho a la intimidad*». Por consiguiente, la Directiva hace una referencia concreta al

5 La rectificación puede hacerse añadiendo comentarios en sentido contrario o utilizando los medios legales apropiados, como, por ejemplo, las vías de recurso

6 Sentencia del Tribunal Europeo de Derechos Humanos en el asunto Amann/Suiza de 16.2.2000, apartado 65: *«[…] el término" vida privada" no debe interpretarse restrictivamente. En especial, el respeto por la vida privada comprende el derecho a establecer y a desarrollar relaciones con otros seres humanos; además, no hay ninguna razón de principio que justifique la exclusión de actividades de una naturaleza de profesional o empresarial de la noción de la "vida privada" (véase al Niemietz v. Sentencia de Alemania del 16 de diciembre de 1992, serie A no. 251- B, pags. 33-34, § 29, y la sentencia Halford citada anteriormente, pags. 1015-16, § 42). Esa interpretación amplia se corresponde con la del convenio del Consejo de Europa de 28 de enero de 1981 […]*»

tratamiento de los datos personales en ámbitos distintos del hogar y de la familia, como el del Derecho laboral [artículo 8, apartado 2, letra b)], las condenas penales, las sanciones administrativas o las sentencias en procesos civiles (artículo 8, apartado 5) o la prospección [artículo 14, letra b)]. El Tribunal de Justicia de las Comunidades Europeas[7] ha refrendado este enfoque amplio.

Desde el punto de vista del formato o el soporte en que la información está contenida, el concepto de datos personales incluye la información disponible en cualquier forma, alfabética, numérica, gráfica, fotográfica o sonora, por ejemplo. Desde este punto de vista, el concepto incluye la información conservada en papel, así como la información almacenada en una memoria de ordenador, utilizando un código binario, o en una cinta de video, por ejemplo. Se trata de una consecuencia lógica de la inclusión en su ámbito de aplicación del tratamiento automático de datos personales. En particular, los datos que consisten en sonidos e imágenes están calificados como datos personales desde este punto de vista, en la medida en que pueden contener información sobre una persona. A este respecto, la referencia particular a los datos consistentes en sonidos e imágenes del artículo 33 de la Directiva debe ser entendida como la confirmación de que esta clase de datos entra en efecto en su ámbito de aplicación (siempre y cuando se cumplan las restantes condiciones) y de que la Directiva se aplica a ellos. De hecho, esto entra dentro de la lógica de este artículo que intenta evaluar si las normas de la Directiva proporcionan respuestas legales apropiadas en esos ámbitos. Esto queda aún más claro en el considerando 14, en el que se afirma que «c*onsiderando que, habida cuenta de la importancia que, en el marco de la sociedad de la información, reviste el actual desarrollo de las técnicas para captar, transmitir, manejar, registrar, conservar o comunicar los datos relativos a las personas físicas constituidos por sonido e imagen, la presente Directiva habrá de aplicarse a los tratamientos que afectan a dichos datos*». Por otra parte, para que la información sea considerada como datos personales no es necesario que esté recogida en una base de datos o en un fichero estructurado. También la información contenida en un texto libre en un documento electrónico puede calificarse como datos personales, siempre que se cumplan los otros criterios de la definición de datos personales. El correo electrónico, por ejemplo, contiene datos personales.

Ejemplo nº 2: Banca telefónica:

En las operaciones de banca telefónica, en las que la voz del cliente que da instrucciones al banco se graba en una cinta, las instrucciones grabadas deben ser consideradas como datos personales.

Ejemplo nº 3: Videovigilancia

Las imágenes de personas obtenidas por medio de un sistema de videovigilancia pueden considerarse datos personales en la medida en que esas personas sean reconocibles.

Ejemplo nº 4: Dibujos infantiles

[7] Sentencia del Tribunal de Justicia de las Comunidades Europeas en el asunto C -101/2001(Lindqvist) de 6.11.2003, apartado 24, Rec. 2003 p. I-12971: «*El concepto de "datos personales" que emplea el artículo 3, apartado 1, de la Directiva 95/46 comprende, con arreglo a la definición que figura en el artículo 2, letra a), de dicha Directiva "toda información sobre una persona física identificada o identificable". Este concepto incluye, sin duda, el nombre de una persona junto a su número de teléfono o a otra información relativa a sus condiciones de trabajo o a sus aficiones*».

Como resultado de una prueba neuropsiquiátrica practicada a una niña en el contexto de un procedimiento judicial sobre su custodia se presentó un dibujo suyo en el que representaba a su familia. El dibujo proporciona información sobre el estado de ánimo de la niña y sus sentimientos con respecto a los diferentes miembros de su familia. Como tal, podría entrar en la categoría de «datos personales». En efecto, el dibujo revela información relativa a la niña (su estado de salud desde un punto de vista psiquiátrico) así como a, por ejemplo, los comportamientos de su padre y de su madre. En consecuencia, los padres pueden ejercer en este caso su derecho de acceso a esta información concreta.

En este punto cabe hacer una referencia especial a los datos biométricos. Estos datos pueden definirse como propiedades biológicas, características fisiológicas, rasgos de la personalidad o tics, que son, al mismo tiempo, atribuibles a una sola persona y mensurables, incluso si los modelos utilizados en la práctica para medirlos técnicamente implican un cierto grado de probabilidad. Ejemplos típicos de datos biométricos son los que proporcionan las huellas dactilares, los modelos retinales, la estructura facial, las voces, pero también la geometría de la mano, las estructuras venosas e incluso determinada habilidad profundamente arraigada u otra característica del comportamiento (como la caligrafía, las pulsaciones, una manera particular de caminar o de hablar, etc.).

Una particularidad de los datos biométricos es que se les puede considerar tanto como *contenido* de la información sobre una determinada persona (Fulano tiene estas huellas dactilares) como un elemento para *vincular* una información a una determinada persona (este objeto lo ha tocado alguien que tiene estas huellas dactilares y estas huellas dactilares corresponden a Fulano; por lo tanto Fulano ha tocado este objeto). Como tales, pueden servir de «identificadores». En efecto, al corresponder a una única persona, los datos biométricos pueden utilizarse para identificar a esa persona. Este carácter dual también se da en el caso de los datos sobre el ADN, que proporcionan información sobre el cuerpo humano y permiten la identificación inequívoca de una, y sólo una, persona.

Las muestras de tejido humano (al igual que las muestras de sangre) son fuentes a partir de las cuales se extraen datos biométricos, pero no son en sí mismas datos biométricos (como, por ejemplo, un modelo de huellas dactilares es un dato biométrico, pero no así un dedo). Por lo tanto, la extracción de información de las muestras supone la obtención de datos personales, a los que se aplican las normas de la Directiva. La obtención, el almacenamiento y el uso de muestras de tejido pueden estar sujetos a un conjunto de normas diferentes[8].

2. SEGUNDO COMPONENTE: «SOBRE»

Este componente de la definición es crucial, ya que es muy importante determinar con precisión cuáles son las relaciones, los vínculos, que importan y cómo distinguirlos.

De modo general, se puede considerar que la información versa «sobre» una persona cuando se refiere a ella.

[8] Véase la Recomendación. Rec (2006)4 del Comité de Ministros del Consejo de Europa a los Estados miembros sobre la investigación con material biológico de origen humano, de 15.3.2006.

En muchas ocasiones, esa relación puede establecerse fácilmente. Por ejemplo, los datos incluidos en el fichero personal de una persona guardado en el departamento de personal de su empresa están claramente relacionados con su situación como empleado de dicha empresa. Otro tanto sucede con los datos sobre los resultados de las pruebas médicas a las que se ha sometido una persona, recogidos en su historial médico, o las imágenes filmadas en video de una persona con ocasión de una entrevista.

Pueden citarse otras situaciones, aunque no siempre resulte tan evidente como en los casos citados anteriormente establecer que la información versa «sobre» una persona concreta.

En algunas ocasiones, la información que proporcionan los datos se refiere no tanto a personas como a objetos. Esos objetos suelen pertenecer a alguien, o pueden estar bajo la influencia de una persona o ejercer una influencia sobre ella o pueden tener una cierta proximidad física o geográfica con personas o con otros objetos. En esos casos, sólo indirectamente puede considerarse que la información se refiere a esas personas u objetos.

Ejemplo nº 5: Valor de una vivienda

El valor de una vivienda es información sobre un objeto. A todas luces, las normas sobre protección de datos no se aplicarán cuando esa información se utilice únicamente para ilustrar el nivel de precios de la vivienda en una determinada zona. Sin embargo, si se dan determinadas circunstancias esa información también debe considerarse como un dato personal. En efecto, la vivienda es un activo de su propietario y, como tal, se tendrá en cuenta, por ejemplo, a la hora de calcular los impuestos que deberá pagar esa persona. En este contexto, es incuestionable que tal información debe considerarse como datos personales.

Un análisis similar puede aplicarse cuando los datos se refieren en primera instancia a procesos o hechos, como por ejemplo el funcionamiento de una máquina cuando es necesaria la intervención humana. Bajo determinadas circunstancias, esta información también puede considerarse información «sobre» una persona.

Ejemplo nº 6: Cuaderno de revisiones de un automóvil

El cuaderno en el que un mecánico o un garaje anotan las revisiones pasadas por un automóvil contiene información sobre éste: kilometraje, fechas de las revisiones, problemas técnicos y estado de conservación. Esta información se asocia en el cuaderno a una matrícula y a un número de motor que, a su vez, pueden vincularse a su propietario. En los casos en que el garaje establezca una conexión entre el vehículo y su dueño a efectos de facturación, la información versará «sobre» el dueño o el conductor. Si se establece una relación con el mecánico que trabajó en el coche con objeto de determinar su productividad, esta información también versará «sobre» el mecánico.

El Grupo de trabajo ya se ocupó anteriormente de la cuestión de cuándo puede considerarse que una información versa «sobre» una persona. En el marco de sus debates sobre los problemas de protección de datos planteados por las etiquetas RFID, el Grupo de trabajo señaló que un «*dato se refiere a una persona si hace referencia a*

su identidad, sus características o su comportamiento o si esa información se utiliza para determinar o influir en la manera en que se la trata o se la evalúa»[9].

Teniendo en cuenta los casos mencionados anteriormente, y siguiendo la misma línea de razonamiento, podría afirmarse que para considerar que los datos versan «sobre» una persona debe haber un elemento **«contenido»** o un elemento **«finalidad»** o un elemento **«resultado»**.

El elemento **«contenido»** está presente en aquellos casos en que - de acuerdo con lo que una sociedad suele general y vulgarmente entender por la palabra «sobre» - se proporciona información sobre una persona concreta, independientemente de cualquier propósito que puedan abrigar el responsable del tratamiento de los datos o un tercero, o de la repercusión de esa información en el interesado. La información versa «sobre» una persona cuando «se refiere» a esa persona, lo que debe ser evaluado teniendo en cuenta todas las circunstancias que rodean el caso. Por ejemplo, los resultados de un análisis médico se refieren claramente al paciente, o la información contenida en el expediente de una empresa bajo el nombre de determinado cliente se refiere claramente a él. De la misma manera, la información contenida en una etiqueta RFID o en un código de barras incorporados al documento de identidad de una determinada persona se refiere a esa persona, como en los futuros pasaportes que llevarán incorporados un microprocesador RFID.

También la presencia de un elemento **«finalidad»** puede ser lo que determine que la información verse «sobre» determinada persona. Se puede considerar que ese elemento **«finalidad»** existe cuando los datos se utilizan o es probable que se utilicen, teniendo en cuenta todas las circunstancias que rodean el caso concreto, con la finalidad de evaluar, tratar de determinada manera o influir en la situación o el comportamiento de una persona.

[9] Documento nº WP 105 del Grupo de trabajo: «Documento de trabajo sobre las cuestiones relativas a la protección de datos relacionadas con la tecnología RFID», adoptado el 19.1.2005, p. 8.

Ejemplo nº 7: Registro de llamadas de un teléfono

El registro de llamadas de un teléfono de una empresa proporciona información sobre las llamadas realizadas desde ese teléfono conectado a una determinada línea telefónica. Esa información puede ponerse en relación con otras informaciones. Por una parte, la línea se ha puesto a disposición de la empresa, la cual está obligada contractualmente a abonar las llamadas. Durante la jornada laboral, el terminal telefónico está bajo el control de un determinado trabajador de la empresa y se supone que es él quien realiza las llamadas. El registro de llamadas también puede proporcionar información sobre las personas a las que se ha llamado. Además, el teléfono puede ser utilizado por cualquier persona que tenga acceso a los locales en ausencia del trabajador responsable (por ejemplo por el personal de limpieza). Por motivos diferentes, la información sobre el uso de ese teléfono puede relacionarse con la empresa, el trabajador, o el personal de limpieza (por ejemplo, para comprobar la hora en que el personal de limpieza dejó el lugar de trabajo, puesto que en principio deben confirmar a través de una llamada telefónica la hora a la que salen antes de cerrar los locales de la empresa). Hay que mencionar que el concepto de datos personales abarca aquí tanto las llamadas salientes como las entrantes en la medida en que todas ellas contienen información sobre la vida privada, las relaciones sociales o las comunicaciones de las personas.

Estamos ante una tercera categoría de «sobre» cuando existe un elemento de **«resultado»**. A pesar de la ausencia de un elemento de «contenido» o de «finalidad» cabe considerar que los datos versan «sobre» una persona determinada porque, teniendo en cuenta todas las circunstancias que rodean el caso concreto, es probable que su uso repercuta en los derechos y los intereses de determinada persona. Basta con que la persona pueda ser tratada de forma diferente por otras personas como consecuencia del tratamiento de tales datos.

Ejemplo nº 8: Sistema de localización de taxis para optimizar el servicio, con repercusiones para los taxistas.

Una empresa de taxis pone en funcionamiento un sistema de localización por satélite gracias al cual puede saber en tiempo real la posición de los taxis libres. La finalidad del tratamiento de esta información es proporcionar un mejor servicio y ahorrar combustible, asignando a cada cliente que solicita un taxi el vehículo más cercano a la dirección en la que se encuentra. En realidad los datos que necesita el sistema son los relativos a los vehículos, no los que se refieren a los conductores. La finalidad del tratamiento no consiste en evaluar el rendimiento de los taxistas a través de, por ejemplo, su capacidad para elegir los mejores itinerarios. Sin embargo, el sistema permite controlar el rendimiento de los taxistas y comprobar si respetan los límites de velocidad, buscan itinerarios apropiados, están al volante o descansando fuera del vehículo, etc. Así pues, puede repercutir de manera importante en estos individuos y, por lo tanto, cabe considerar que los datos también se refieren a personas físicas. El tratamiento de esos datos debería estar sujeto a las normas de protección de datos.

Estos tres elementos (contenido, finalidad y resultado) deben considerarse como condiciones alternativas y no acumulativas. En especial, cuando exista el elemento de contenido, no hay ninguna necesidad de que también aparezcan los otros elementos para considerar que la información se refiere a una persona física. Corolario de lo

anterior es que una misma información puede referirse al mismo tiempo a diversas personas, en función del elemento que esté presente en relación con cada una de ellas. Una misma información puede referirse a Fulano debido al elemento de «contenido» (los datos se refieren sin lugar a dudas a Fulano) y a Mengano si consideramos el elemento de «finalidad» (la información se utilizará para tratar a Mengano de determinada manera), pero también se refiere a Zutano debido al elemento de «resultado» (es probable que la información repercuta en los derechos e intereses de Zutano). Esto también significa que no es necesario que los datos «se centren» en una persona determinada para considerar que se refieren a ella. Del análisis anterior se desprende que a la pregunta de si los datos se refieren a determinada persona hay que contestar, analizando cada dato, en función de sus características. De igual manera, el hecho de que una información pueda referirse a diversas personas debe tenerse en cuenta al aplicar las disposiciones sustantivas (por ejemplo, el alcance del derecho de acceso).

Ejemplo nº 9: Información contenida en las actas de una reunión

Un ejemplo de la necesidad de realizar el análisis de cada dato por separado lo tenemos en la información contenida en el acta de una reunión cualquiera, en la que consta que participaron en ella Fulano, Mengano y Zutano; las declaraciones formuladas por Fulano y Mengano; y un informe resumido de los debates mantenidos sobre determinados asuntos realizado por el redactor de las actas, Zutano. Sólo cabe considerar como datos personales sobre Fulano los de que asistió a la reunión en un determinado momento y lugar e hizo ciertas declaraciones. La presencia en la reunión de Mengano, sus declaraciones y el relato de los debates reflejados en el acta por Zutano NO son datos personales sobre Fulano. Esto es así aunque esa información esté contenida en el mismo documento e incluso aunque fuera Fulano el que sacó a relucir el tema sobre el que se debatió en la reunión. Por lo tanto estos últimos datos están excluidos del derecho de Fulano a acceder a sus propios datos personales. Si, y en qué medida, esos datos pueden considerarse datos personales sobre Mengano y Zutano, habrá que determinarlo por separado utilizando el método de análisis descrito anteriormente.

3. TERCER COMPONENTE: [PERSONA FÍSICA] «IDENTIFICADA O IDENTIFICABLE»

La Directiva requiere que la información se refiera a una persona física «identificada o identificable». Ello suscita las siguientes consideraciones.

De modo general, se puede considerar «identificada» a una persona física cuando, dentro de un grupo de personas, se la «distingue» de todos los demás miembros del grupo. Por consiguiente, la persona física es «identificable» cuando, aunque no se la haya identificado todavía, sea posible hacerlo (que es el significado del sufijo «ble»). Así pues, esta segunda alternativa es, en la práctica, la condición suficiente para considerar que la información entra en el ámbito de aplicación del tercer componente.

La identificación se logra normalmente a través de datos concretos que podemos llamar «identificadores» y que tienen una relación privilegiada y muy cercana con una determinada persona. Cabe citar como ejemplos su apariencia exterior, es decir su altura, el color del cabello, la ropa, etc. o una cualidad de la persona que no puede percibirse inmediatamente, como su profesión, el cargo que ocupa, su nombre, etc. La Directiva menciona esos «identificadores» en la definición de «datos personales» del

artículo 2 cuando establece que «*se declarará 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*».

«Directa» o «indirectamente» identificable

Esta idea se aclara aún más en los comentarios a los artículos de la propuesta modificada de la Comisión, en donde se afirma que *«una persona puede ser identificada directamente por su nombre y apellidos o indirectamente por un número de teléfono, la matrícula de un coche, un número de seguridad social, un número de pasaporte o por una combinación de criterios significativos (edad, empleo, domicilio, etc.),que haga posible su identificación al estrecharse el grupo al que pertenece.*» Los términos de esta declaración indican claramente que el que determinados identificadores se consideren suficientes para lograr la identificación es algo que depende del contexto de la situación de que se trate. Un apellido muy común no bastará para identificar a una persona - es decir, para aislarla – dentro del conjunto de la población de un país, mientras que es probable que permita la identificación de un alumno dentro de una clase. Incluso una información auxiliar, como, por ejemplo, «el hombre que lleva un traje negro», puede identificar a alguno de los transeúntes que esperan en un semáforo. Así pues, el que se identifique o no a la persona a la que se refiere una información depende de las circunstancias concretas del caso.

Por lo que se refiere a la expresión personas «directamente» identificadas o identificables, **el nombre y apellidos** de una persona es efectivamente el identificador más común y, en la práctica, el concepto de «persona identificada » implica muy a menudo una referencia a sus apellidos.

En algunas ocasiones, para establecer con toda certeza esta identidad, hay que combinar el nombre y apellidos de la persona con otros datos (fecha de nacimiento, nombres de los padres, dirección o una fotografía de su rostro) para evitar toda confusión con otras personas del mismo nombre y apellidos. Por ejemplo, puede considerarse que la información de que Fulano debe una cierta suma de dinero hace referencia a una persona identificada porque está ligada al nombre y apellidos de esa persona. El nombre y apellidos de una persona es una información que revela que ésta utiliza esa combinación de letras y sonidos para identificarse y para que la identifiquen otras personas con las que establece relaciones. El nombre y apellidos de una persona también pueden ser el punto de partida para obtener información sobre el lugar en el que vive o se la puede encontrar, o sobre sus familiares (a través de sus apellidos) y sobre toda una serie de relaciones jurídicas y sociales vinculadas a ese nombre y apellidos (expediente académico, expediente médico, cuentas bancarias, etc.). Se puede incluso conocer la apariencia física de la persona si su fotografía se asocia con su nombre y apellidos. Todos estos nuevos datos ligados al nombre y apellidos nos permiten centrarnos en un individuo de carne y hueso. Así pues, a través de los identificadores la información original se asocia con una persona física que puede ser distinguida de otros individuos.

Por su parte, cuando hablamos de «indirectamente» identificadas o identificables, nos estamos refiriendo en general al fenómeno de las «combinaciones únicas», sean éstas pequeñas o grandes. En los casos en que, a primera vista, los identificadores disponibles no permiten singularizar a una persona determinada, ésta aún puede ser «identificable», porque esa información combinada con otros datos (tanto si el

responsable de su tratamiento tiene conocimiento de ellos como si no) permitirá distinguir a esa persona de otras. Aquí es donde la Directiva se refiere a «uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social». Algunas de esas características son tan únicas que permiten identificar a una persona sin esfuerzo (el «actual Presidente del Gobierno de España »), pero una combinación de detalles pertenecientes a distintas categorías (edad, origen regional, etc.) también puede ser lo bastante concluyente en algunas circunstancias, en especial si se tiene acceso a información adicional de determinado tipo. Este fenómeno ha sido estudiado ampliamente por los estadísticos, siempre dispuestos a evitar cualquier quebrantamiento de la confidencialidad.

Ejemplo nº 10: Información dispersa en la prensa

Se publica un artículo de prensa sobre un antiguo asunto penal que en su día suscitó mucho interés. En este artículo no se da ninguno de los identificadores tradicionales, en especial ni la identidad ni el lugar de nacimiento de ninguna de las personas involucradas.

No parece excesivamente difícil obtener información adicional que nos permita descubrir cuáles son las personas más directamente implicadas en el asunto, por ejemplo, echando un vistazo a la prensa de la época en que se desarrollaron los acontecimientos. De hecho, no es inconcebible que alguien consulte los periódicos de la época o dé otros pasos que muy probablemente le proporcionen los nombres u otros identificadores de las personas a las que veladamente se hace referencia en el artículo. Por lo tanto, parece justificado considerar el tipo de información al que se hace referencia en este ejemplo como «información sobre personas identificables» y, por tanto, como «datos personales».

Al llegar a este punto, conviene señalar que, si bien la identificación a través del nombre y apellidos es en la práctica lo más habitual, esa información puede no ser necesaria en todos los casos para identificar a una persona. Así puede suceder cuando se utilizan otros «identificadores» para singularizar a alguien. Efectivamente, los ficheros informatizados de datos personales suelen asignar un identificador único a las personas registradas para evitar toda confusión entre dos personas incluidas en el fichero. También en Internet, las herramientas de control de tráfico permiten identificar con facilidad el comportamiento de una máquina y, por tanto, la del usuario que se encuentra detrás. Así pues, se unen las diferentes piezas que componen la personalidad del individuo con el fin de atribuirle determinadas decisiones. Sin ni siquiera solicitar el nombre y la dirección de la persona es posible incluirla en una categoría, sobre la base de criterios socioeconómicos, psicológicos, filosóficos o de otro tipo, y atribuirle determinadas decisiones puesto que el punto de contacto del individuo (un ordenador) hace innecesario conocer su identidad en sentido estricto. En otras palabras, la posibilidad de identificar a una persona ya no equivale necesariamente a la capacidad de poder llegar a conocer su nombre y apellidos. La definición de datos personales refleja este hecho[10].

[10] Informe elaborado para el Comité T-PD del Consejo de Europa por el Sr. Yves Poullet y su equipo sobre la aplicación de los principios sobre protección de datos a las redes mundiales de telecomunicación, punto 2.3.1, T-PD(2004) 04 final.

El Tribunal de Justicia de las Comunidades Europeas se ha pronunciado en ese sentido al considerar que *«la conducta que consiste en hacer referencia, en una página web, a diversas personas y en identificarlas por su nombre o por otros medios, como su número de teléfono o información relativa a sus condiciones de trabajo y a sus aficiones, constituye un tratamiento […] de datos personales en el sentido del artículo 3, apartado 1, de la Directiva 95/46.»* [11]

Ejemplo nº 11: Solicitantes de asilo

A unos solicitantes de asilo que ocultan su verdadera identidad y que se encuentran en un centro de acogida se les ha asignado un número de código a efectos administrativos. Ese número servirá de identificador, de modo que diversos datos referentes a la estancia de cada solicitante de asilo en la institución se asociarán a él. Además mediante una fotografía u otros indicadores biométricos, ese número de código se conectará de manera directa e inmediata a una persona física, lo que hará posible que se le distinga de otros solicitantes de asilo y se le atribuyan diferentes datos, que se referirán a una persona física «identificada».

El Artículo 8, apartado 7, de la Directiva también establece que los «*Estados miembros determinarán las condiciones en las que un número nacional de identificación o cualquier otro medio de identificación de carácter general podrá ser objeto de tratamiento*». Conviene señalar el sentido de esta disposición, que no contiene ninguna indicación particular sobre el tipo de condiciones que deben adoptar los Estados miembros, pero que se inscribe en el artículo que trata de los datos sensibles. El considerando 33 se refiere a esta clase de datos como los *«datos que por su naturaleza puedan atentar contra las libertades fundamentales o la intimidad*». Entra dentro de lo razonable pensar que el legislador puede haber sentido una preocupación similar con respecto a los números nacionales de identificación debido a su gran capacidad para relacionar fácil e inequívocamente diferentes datos sobre una determinada persona.

Medios de identificación

El considerando 26 de la Directiva presta una atención particular al término «identificable» al decir que «*para 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*». Esto significa que la mera e hipotética posibilidad de singularizar a un individuo no es suficiente para considerar a la persona como «identificable». Si, teniendo en cuenta *«el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona»*, no existe esa posibilidad o es insignificante, la persona no debe ser considerada como «identificable» y la información no debe catalogarse como «datos personales» El criterio del *«conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona*» debe tener especialmente en cuenta todos los factores en juego. Lo costoso de la identificación es un factor, pero no el único. La finalidad del tratamiento, la manera en que el tratamiento está estructurado, el rédito que espera obtener el responsable del tratamiento, los intereses individuales en juego, así como el riesgo de que se produzcan disfunciones organizativas (por ejemplo, un quebrantamiento del deber de confidencialidad) y los fracasos técnicos son todos ellos elementos que deben tenerse en

[11] Sentencia del Tribunal de Justicia de las Comunidades Europeas en el asunto C -101/2001(Lindqvist) de 6.11.2003, apartado 27, Rec. 2003 p. I-12971.

cuenta. Por otra parte, se trata de una prueba dinámica, por lo que debe tenerse en cuenta el grado de avance tecnológico en el momento del tratamiento y su posible desarrollo en el período durante el cual se tratarán los datos. Puede que la identificación no sea factible hoy con el conjunto de los medios que puedan ser razonablemente utilizados en la actualidad. Si lo previsto es que los datos se conserven durante un mes, puede que no sea factible adelantar la identificación para que esté terminada dentro del «período de vida» de la información y, por lo tanto, esa información no debe considerarse como datos personales. Ahora bien, si el período de conservación previsto es de diez años, el responsable del tratamiento debe barajar la posibilidad de que la identificación pueda producirse al cabo de nueve años, con lo que adquiriría en ese momento la categoría de datos personales. Es preciso que el sistema sea capaz de adaptarse a los progresos tecnológicos a medida que éstos se produzcan y que introduzca las medidas técnicas y organizativas apropiadas a su debido tiempo.

Ejemplo nº 12: Publicación de unas radiografías con indicación del nombre del paciente al que pertenecen

Una radiografía de una señora se publica en un diario científico junto con su nombre de pila, muy poco corriente. El nombre de la persona unido al hecho de que sus parientes y conocidos saben que padece una determinada enfermedad hace posible que algunas personas puedan saber de quién se trata, lo que convierte a la radiografía en un dato personal.

Ejemplo nº 13: Datos de investigación farmacéutica

Hospitales o médicos a título individual transmiten datos de los expedientes médicos de sus pacientes a una empresa con fines de investigación médica. No se facilita el nombre de los pacientes, sino solamente unos números de serie atribuidos de forma aleatoria a cada caso clínico para garantizar un cierto grado de coherencia y evitar confusiones entre los datos de los diferentes pacientes. Sólo los médicos, sometidos al secreto profesional, conocen su identidad. Los datos transmitidos no contienen ninguna información adicional que permita, a través de su combinación, la identificación de los pacientes. Además, se han tomado todas las medidas, legales, técnicas u organizativas, para evitar que los interesados sean identificados o puedan llegar a serlo. En estas circunstancias, una autoridad de protección de datos puede considerar que al procesar esos datos la empresa farmacéutica no utiliza medios que puedan razonablemente utilizarse para identificar a los interesados.

Un factor importante, como se dijo anteriormente, para evaluar el «conjunto de los medios que puedan ser razonablemente utilizados» para identificar a las personas será la finalidad perseguida por el responsable del tratamiento al llevarlo a cabo. Las autoridades nacionales de protección de datos se han enfrentado a casos en los que el responsable del tratamiento sostenía que sólo se habían tratado informaciones dispersas, sin referencias a nombres u otros identificadores directos, y abogaba porque los datos no se considerasen como personales y no estuvieran sujetos a las normas de protección de los datos. Y, sin embargo, el tratamiento de esa información sólo cobraba sentido si permitía la identificación de individuos concretos y su tratamiento de una manera determinada. En estos casos, en los que la finalidad del tratamiento implica la identificación de personas, puede asumirse que el responsable del tratamiento o cualquier otra persona implicada tiene o puede tener medios que «puedan ser razonablemente utilizados», para identificar al interesado. De hecho, sostener que las personas físicas no son identificables, cuando la finalidad del tratamiento es precisamente identificarlos, sería una contradicción flagrante.

Por lo tanto, debe considerarse que la información se refiere a personas físicas identificables y el tratamiento debe estar sujeto a las normas de protección de datos.

Ejemplo nº 14: Videovigilancia

Esto es especialmente pertinente en el ámbito de la videovigilancia, en el que los responsables del tratamiento con frecuencia sostienen que la identificación sólo se produce en un pequeño porcentaje de casos y que, por lo tanto, hasta que no se produce la identificación en esos pocos casos, realmente no se trata ningún dato personal. Como la finalidad de la videovigilancia es, sin embargo, identificar a las personas que aparecen en las imágenes de vídeo en todos aquellos casos en los que esa identificación es considerada necesaria por el responsable del tratamiento, hay que considerar el uso del sistema en sí como tratamiento de datos sobre personas identificables, aun cuando algunas de las personas filmadas no sean identificables en la práctica.

Ejemplo nº 15: Direcciones IP dinámicas

El Grupo de trabajo considera las direcciones IP como datos sobre una persona identificable. En ese sentido ha declarado que «*los proveedores de acceso a Internet y los administradores de redes locales pueden identificar por medios razonables a los usuarios de Internet a los que han asignado direcciones IP, pues registran sistemáticamente en un fichero la fecha, la hora, la duración y la dirección IP dinámica asignada al usuario de Internet. Lo mismo puede decirse de los proveedores de servicios de Internet que mantienen un fichero registro en el servidor HTTP. En estos casos, no cabe duda de que se puede hablar de datos de carácter personal en el sentido de la letra a) del artículo 2 de la Directiva*»[12].

Especialmente en aquellos casos en los que el tratamiento de direcciones IP se lleva a cabo con objeto de identificar a los usuarios de un ordenador (por ejemplo, el realizado por los titulares de los derechos de autor para demandar a los usuarios por violación de los derechos de propiedad intelectual), el responsable del tratamiento prevé que los «medios que pueden ser razonablemente utilizados» para identificar a las personas pueden obtenerse, por ejemplo, a través de los tribunales competentes (de otro modo la recopilación de información no tiene ningún sentido), y por lo tanto la información debe considerarse como datos personales.

Un caso particular sería el de algunos tipos de direcciones IP que en determinadas circunstancias y por diversas razones técnicas y organizativas no permiten realmente la identificación del usuario. Así sucede, por ejemplo, con las direcciones IP atribuidas a un ordenador instalado en un cibercafé, en el que no se pide identificación alguna a los clientes. En este caso, puede argüirse que los datos recogidos sobre el uso de un determinado ordenador «X» durante una determinada franja horaria no permiten la identificación del usuario con medios razonables y, por lo tanto, no son datos personales. Sin embargo cabe señalar que, muy probablemente, los prestatarios de servicios de Internet no sabrán si la dirección IP en cuestión permite la identificación o no, y tratarán los datos asociados a ese IP de la misma manera que tratarían la información asociada a las direcciones IP de los usuarios debidamente registrados e identificables. Así pues, a menos que el prestatario de servicios de Internet sepa con absoluta certeza que los datos corresponden a usuarios que no pueden ser identificados,

[12] Documento de trabajo WP 37: Privacidad en Internet: - Enfoque comunitario integrado de la protección de datos en línea adoptado el 21.11.2000.

tendrá que tratar toda información IP como datos personales, para guardarse las espaldas.

Ejemplo nº 16: Daños causados por *graffiti*

Los vehículos de pasajeros de una empresa de transporte sufren repetidamente daños al ser objeto de pintadas («graffiti») que ensucian sus carrocerías. Para evaluar los daños causados y facilitar el ejercicio de demandas legales contra los autores de las pintadas, la empresa elabora un fichero con información sobre las circunstancias en que se produjeron los daños e imágenes de los bienes dañados y de las «etiquetas» o «firmas» de sus autores. En el momento de introducir la información en el fichero, se desconocen los causantes del daño y a quién pertenece la «firma». Cabe dentro de lo posible que nunca se conozcan estos datos. Sin embargo, la finalidad del tratamiento es precisamente identificar a los individuos a quienes se refiere la información como los causantes del daño, a fin de poder ejercer demandas legales contra ellos. Ese tratamiento tiene sentido si el responsable del tratamiento considera «razonablemente probable» que un día cuente con los medios para identificar a los autores de las pintadas. La información contenida en los dibujos debe entenderse referida a individuos «identificables», la información incluida en el fichero como «datos personales» y el tratamiento debe estar sujeto a las normas de protección de datos, que legitiman el tratamiento en determinadas circunstancias y siempre que se respeten una serie de salvaguardias.

En los casos en que la identificación del interesado no entre en la finalidad del tratamiento, las medidas técnicas para evitar la identificación tienen un papel muy importante. Adoptar las medidas técnicas y organizativas adecuadas de acuerdo con los conocimientos técnicos existentes para proteger los datos contra la identificación puede constituir la clave para considerar que las personas no son identificables, teniendo en cuenta *el conjunto de medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona,* para identificarlas. En este caso, la aplicación de esas medidas no es *consecuencia* de una obligación jurídica impuesta por el artículo 17 de la Directiva (que únicamente se aplica si la información se considera como datos personales a primera vista), sino *una condición* para que precisamente la información no se considere como datos personales y su tratamiento no esté sujeto a la Directiva.

Datos relativos a seudónimos

La utilización de seudónimos («*seudonimización*»**)** se utiliza para ocultar identidades. La finalidad del uso de seudónimos es poder recopilar más datos sobre una misma persona sin necesidad de conocer su identidad. Su uso es especialmente pertinente en los ámbitos estadístico e investigador.

La «*seudonimización*» pueden realizarse de forma que quede un rastro entre el seudónimo y la identidad con la que se corresponde, utilizando listas de correspondencias o algoritmos criptográficos bidireccionales. Ocultar identidades también puede hacerse sin dejar rastro alguno que permita vincular un seudónimo con una identidad, utilizando, por ejemplo, la criptografía unidireccional, que en general crea datos anónimos.

La eficacia del procedimiento de «*seudonimización*» depende de varios factores (en qué etapa se utiliza, su grado de seguridad contra el rastreo inverso, el tamaño de la población en la que se oculta al individuo, la capacidad de vincular transacciones o documentos

individuales con una misma persona, etc.). Los seudónimos deben ser aleatorios e imprevisibles. El número de seudónimos posibles debe ser tan amplio que no exista la posibilidad de seleccionar aleatoriamente el mismo seudónimo dos veces. En caso de que sea necesario un alto nivel de seguridad, el grupo de posibles seudónimos debe ser por lo menos igual a la gama de valores de funciones criptográficas numéricas seguras[13].

Los datos de una «*seudonimización*» rastreable pueden considerarse información sobre personas físicas *indirectamente identificables*. De hecho, la utilización de un seudónimo supone la posibilidad de seguir un rastro hasta llegar a la identidad de la persona, aunque sólo en condiciones previamente definidas. En ese caso, aunque son aplicables las normas de protección de datos, los peligros para los individuos en lo referente al tratamiento de esa información identificable indirectamente son la mayoría de las veces muy pequeños, lo que justifica que esas normas se apliquen de manera más flexible que si se tratara de información sobre individuos directamente identificables.

Datos cifrados

Los datos cifrados son un ejemplo clásico de «*seudonimización*». La información contenida en esos datos se refiere a un individuo al que se asigna un código cifrado, mientras que la clave para descifrarlos, es decir para establecer la correspondencia entre el código y los identificadores habituales de la persona (nombre, fecha de nacimiento, dirección, etc.) se guardan por separado.

Ejemplo nº 17: Datos estadísticos no agregados

Un ejemplo que ilustra la importancia que reviste tener en cuenta todas las circunstancias a fin de evaluar si los medios para identificar a una persona podrán ser «razonablemente utilizados» es el de la información personal tratada por los institutos nacionales de estadística («INE»). En una determinada fase de su labor estadística, los INE guardan en forma no agregada información relativa a personas concretas, personas a las que se asigna un código en vez de un nombre (por ejemplo, el individuo con el código X1234 bebe un vaso de vino más de 3 veces por semana). El INE guarda por separado la clave de estos códigos (la lista que asocia los códigos con los nombres de las personas). Cabe dentro de lo *razonablemente posible* que el INE utilice esa clave y, por lo tanto, el conjunto de datos referentes a una persona concreta puede considerarse como datos personales y el INE debe aplicarles las normas de protección de datos. Ahora, imaginemos que una lista con datos sobre los hábitos de consumo de vino de los ciudadanos se envía a la organización nacional de productores de vino para permitirles que apoyen su posición en datos estadísticos. Para determinar si la información contenida en esa lista aún puede considerarse como datos personales, debe evaluarse si los consumidores individuales de vino pueden ser identificados teniendo en cuenta *«el conjunto de medios que puedan razonablemente ser utilizados por el responsable del tratamiento o por cualquier otra persona*».

Si a cada persona física se le ha asignado un único código, siempre existe un riesgo de identificación en caso de que sea posible acceder a la clave utilizada para el cifrado. Por lo tanto, los riesgos de un acceso ilegal desde el exterior, la probabilidad de que

[13] Véase el documento de trabajo «*Privacy-enhancing technologies*» elaborado por el Grupo de trabajo sobre «tecnologías para mejorar la protección de la vida privada» del Comité sobre Aspectos Técnicos y Organizativos de la Protección de los Datos» de los Comisarios para la protección de datos de los estados federados alemanes de (octubre de 1997), publicado en http://ec.europa.eu/justice_home/fsj/privacy/studies/index_en.htm

alguien de la organización remitente - a pesar de estar sujeto al secreto profesional - proporcione la clave *y por ende* la vía para una identificación indirecta, son factores que deben tenerse en cuenta para determinar si las personas pueden ser identificadas teniendo en cuenta *el conjunto de medios que puedan razonablemente ser utilizados por el responsable del tratamiento o por cualquier otra persona* y, por lo tanto, si la información debe considerarse como «datos personales». En caso afirmativo, serán aplicables las normas de protección de datos. Una cuestión diferente es la de que esas normas de protección de datos puedan tener en cuenta el hecho de que los riesgos para los individuos sean reducidos y someter el tratamiento de los datos a condiciones más o menos estrictas, aprovechando la flexibilidad de las normas de la Directiva.

Si, por el contrario, los códigos no son únicos, sino que el mismo número de código (por ejemplo, «123») se utiliza para referirse a personas que viven en distintas ciudades y a datos correspondientes a años diferentes (limitándose a inscribir a una persona dentro de un año y de la muestra de población de una misma ciudad), el responsable del tratamiento o un tercero sólo podrá identificar a una determinada persona si sabe a qué año y a qué ciudad se refieren los datos. Si esta información adicional no consta y no parece que pueda ser razonablemente recuperada, puede considerarse que la información no se refiere a personas identificables y no estaría sujeta a las normas de protección de datos.

Esta clase de datos se utiliza comúnmente en ensayos clínicos con medicamentos. La Directiva 2001/20/CE, de 4 de abril de 2001, sobre la aplicación de buenas prácticas clínicas en la realización de ensayos clínicos de medicamentos de uso humano[14] establece el marco jurídico para llevar a cabo estas actividades. El médico/investigador («investigador») que ensaya los medicamentos recopila la información sobre los resultados clínicos de cada paciente, asignándoles un código. El investigador proporciona la información a la empresa farmacéutica o a otras partes interesadas («patrocinadores») únicamente de forma cifrada, puesto que sólo les interesa la información bioestadística. No obstante, el investigador guarda por separado la clave que permite asociar este código con la información utilizada usualmente para identificar individualmente a los pacientes. Para proteger la salud de los pacientes en caso de que los medicamentos planteen peligros, el investigador está obligado a guardar esta clave, de modo que cada paciente pueda ser identificado y recibir el tratamiento apropiado en caso necesario.

La cuestión que se plantea aquí es saber si se puede considerar que los datos utilizados para el ensayo clínico se refieren a personas físicas «identificables» y están, por lo tanto, sujetos a las normas de protección de datos. Según el análisis descrito anteriormente, para determinar si una persona es identificable se debe tener en cuenta el conjunto de medios que puedan razonablemente ser utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona. En este caso, la identificación de los pacientes (para aplicarles los cuidados apropiados en caso necesario) es una de las finalidades del tratamiento de los datos cifrados. La empresa farmacéutica ha analizado sistemáticamente los medios para el tratamiento de los datos, incluidas las medidas organizativas y sus relaciones con el investigador que guarda la clave, para que la identificación de personas físicas no sólo sea algo que *puede* suceder, sino más bien algo que *debe* suceder en determinadas circunstancias. La identificación de pacientes encaja pues en las finalidades y los medios del tratamiento. En este caso, se puede concluir que esos datos cifrados constituyen información

[14] DO L 121 de 1.5.2001, p. 34.

relativa a personas físicas identificables para todas las partes interesadas en su posible identificación, y deben estar sujetos a las normas de protección de datos. Esto no significa, sin embargo, que cualquier otro responsable del tratamiento de datos que trate el mismo conjunto de datos codificados esté tratando datos personales si dentro del sistema específico en el cual trabajan esos otros responsables se excluye explícitamente la reidentificación y se han tomado a este respecto las medidas técnicas adecuadas.

En otros campos de investigación del mismo proyecto, puede haberse excluido la reidentificación del interesado al diseñar los protocolos y el procedimiento; por ejemplo, porque no se tocan aspectos terapéuticos. Por razones técnicas o de otro tipo, aún puede haber una manera de descubrir a qué persona corresponden determinados datos clínicos, aunque la identificación no esté prevista ni se espere en ningún caso y se hayan adoptado las medidas técnicas adecuadas (por ejemplo, cifrado, comprobación aleatoria irreversible, etc.) para evitar que eso suceda. En este caso, aunque la identificación de determinados interesados pueda producirse a pesar de todos esos protocolos y medidas (debido a circunstancias imprevistas como el descubrimiento accidental de cualidades del interesado que revelen su identidad), no cabe considerar que la información procesada por el responsable original del tratamiento se refiera a personas físicas identificadas o identificables, teniendo en cuenta *el conjunto de medios que puedan razonablemente ser utilizados por el responsable del tratamiento o por cualquier otra persona*. Así pues, el tratamiento de esa información puede no estar sujeto a las disposiciones de la Directiva. Otra cosa distinta sería que el nuevo responsable del tratamiento lograra acceder a información identificable, aquí la información obtenida debería considerarse sin lugar a dudas como «datos personales».

Pregunta más frecuente («FAQ») 14-7 sobre el régimen de puerto seguro

La problemática de los datos cifrados en la investigación farmacéutica se ha abordado en el marco del régimen del puerto seguro[15]. La *FAQ* 14-7 reza así:

FAQ 14 - Productos médicos y farmacéuticos

P.7: El investigador principal codifica siempre los datos de la investigación, en su origen, con una clave única para que no se conozca la identidad de los interesados. Las empresas farmacéuticas que patrocinan la investigación no reciben la clave. El código original sólo lo conoce el investigador, de modo que sólo él puede identificar al sujeto de la investigación en determinadas circunstancias (por ejemplo, cuando es necesario un acompañamiento médico). Una transferencia de datos codificados de esta forma desde la Unión Europea a Estados Unidos de América, ¿constituye una transferencia de datos personales sujeta a los principios de puerto seguro?

R.7: No, no se trata de una transferencia de datos personales sujeta a los mencionados principios.

El Grupo de trabajo considera que esta declaración del sistema de puerto seguro no es contraria al razonamiento descrito anteriormente en pro de considerar esa información como datos personales sujetos a la Directiva. En realidad, esta pregunta no es suficientemente precisa puesto que no aclara a quién y en qué circunstancias se transmiten los datos. El Grupo de trabajo entiende que la pregunta hace referencia al

[15] Decisión de la Comisión 2000/520/CE, de 26.7.2000, DO. L 215/7 de 25.8.2000.

supuesto en que el dato cifrado se transmite a un destinatario en los EE.UU. (por ejemplo, la empresa farmacéutica) que sólo recibe datos cifrados y nunca conocerá la identidad de los pacientes, que es conocida, o será conocida en caso de que sea necesario un tratamiento médico, únicamente por el médico/investigador de la UE, pero nunca por la empresa de los EE.UU.

Datos anónimos

A los efectos de la Directiva, los «datos anónimos» pueden definirse como cualquier información relativa a una persona física que no permita su identificación por el responsable del tratamiento de los datos o por cualquier otra persona, teniendo en cuenta *el conjunto de medios que puedan razonablemente ser utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona*. «Datos *anonimizados*» serán, por lo tanto, los datos anónimos que con anterioridad se referían a una persona identificable, cuya identificación ya no es posible. El considerando 26 también hace referencia a este concepto cuando dice que «*los principios de protección no se aplicarán a aquellos datos hechos anónimos de manera tal que ya no sea posible identificar al interesado*». Una vez más, la decisión sobre si los datos permiten la identificación de una persona y sobre si la información puede considerarse como anónima o no depende de las circunstancias concretas de cada caso, por lo que debe realizarse un análisis caso por caso, en el que habrá que prestar especial atención a hasta qué punto cabe considerar razonablemente posible que se utilicen los medios para identificar a dicha persona, tal como se describe en el considerando 26. Esto es particularmente importante en el caso de la información estadística, puesto que a pesar de que ésta pueda facilitarse en forma de datos agregados, la muestra original puede no ser suficientemente amplia y otros datos pueden permitir la identificación de personas físicas.

Ejemplo nº 18: Encuestas estadísticas y combinación de información dispersa

Con independencia de su obligación general de respetar las normas de protección de datos, para asegurar el anonimato de las encuestas estadísticas, los estadísticos están sujetos a un deber específico de secreto profesional, en virtud del cual no pueden publicar datos que no sean anónimos. Esa prohibición les obliga a publicar datos estadísticos agregados que no puedan atribuirse a una persona identificada. Esta norma es particularmente importante en lo que atañe a la publicación de datos del censo. Se debería establecer un umbral, adaptado a cada situación concreta, por debajo del cual la identificación de las personas a las que se refieren los datos se considere factible. Si un determinado criterio parece conducir a la identificación en una categoría dada de personas, aunque sea grande (es decir, si solamente un médico opera en una ciudad de 6 000 habitantes), debe abandonarse completamente ese criterio «discriminatorio» o añadir otros criterios para «difuminar» los resultados que apunten a una persona dada a fin de garantizar el secreto estadístico.

Ejemplo nº 19: Emisión de imágenes captadas por un sistema de videovigilancia

Un comerciante que ha instalado un sistema de videovigilancia en su tienda. exhibe en su tienda imágenes de unos ladrones obtenidas por medio del sistema de videovigilancia. Después de la intervención de la policía, difumina los rostros de los ladrones, oscureciéndolos. Sin embargo, incluso tras esta operación, aún existe la posibilidad de que las personas que aparecen en las imágenes puedan ser reconocidas

por sus amigos, parientes o vecinos, debido a que, por ejemplo, su complexión física, su corte de pelo y su ropa siguen siendo reconocibles.

4. CUARTO COMPONENTE: «PERSONA FÍSICA»

La protección proporcionada por las normas de la Directiva se aplica a las personas físicas, es decir, a los seres humanos. El derecho a la protección de los datos personales es, en ese sentido, universal sin circunscribirse a los nacionales o residentes en determinado país. El considerando 2 de la Directiva así lo establece explícitamente al afirmar que «*los sistemas de protección de datos están al servicio del hombre*» y que «*deben, cualquiera que sea la nacionalidad o la residencia de las personas físicas, respetar las libertades y derechos fundamentales*».

Al concepto de persona física se hace referencia en el artículo 6 de la Declaración Universal de los Derechos Humanos, en el que se afirma que «*todo ser humano tiene derecho, en todas partes, al reconocimiento de su personalidad jurídica.*» Los ordenamientos jurídicos de los Estados miembros, en general en su orden civil, delimitan con mayor precisión el concepto de personalidad de los seres humanos, entendida como la capacidad de que están dotadas las personas para ser sujetos de relaciones jurídicas, desde su nacimiento hasta su muerte. Los datos personales son, por lo tanto, datos relativos a *seres vivos* identificados o identificables en principio. Esto plantea varias cuestiones a efectos del presente análisis.

Datos sobre personas fallecidas

En principio, la información relativa a personas fallecidas no se debe considerar como datos personales sujetos a las normas de la Directiva, ya que los difuntos dejan de ser personas físicas para el Derecho civil. Sin embargo, en determinados casos los datos de los difuntos aún pueden recibir indirectamente una cierta protección.

En primer lugar, el responsable de los datos quizá no pueda saber a ciencia cierta si la persona a la que se refieren los datos aún está viva o ha fallecido. O aunque pueda saberlo, la información sobre los muertos puede tratarse exactamente de la misma manera que la relativa a los vivos. Como el responsable de los datos está sujeto a las obligaciones sobre protección de datos que impone la Directiva en lo referente a los datos sobre las personas vivas, probablemente le resulte más fácil en la práctica tratar también los datos sobre los muertos de la misma manera, en vez de distinguir entre los dos grupos de datos.

En segundo lugar, la información sobre personas fallecidas también puede hacer referencia a personas vivas. Por ejemplo, la información de que Menganita, ya fallecida, era portadora del gen de la hemofilia indica que su hijo Fulano también puede sufrir la misma enfermedad, pues dicha enfermedad está ligada a un gen contenido en el cromosoma X. Así pues, cuando se considere que la información proporcionada por los datos sobre una persona fallecida también se refiere al mismo tiempo a una persona viva, constituyendo datos personales sujetos a la Directiva, los datos personales del difunto podrán disfrutar indirectamente del amparo de las normas de protección de datos.

En tercer lugar, la información sobre personas fallecidas puede estar sujeta a una protección específica proporcionada por normas distintas de las de protección de datos, que establezcan las líneas de lo que algunos llaman la «*personalidad pretérita*»**.** La

obligación de confidencialidad del personal médico no termina con la muerte del paciente. La legislación nacional sobre el derecho a la propia imagen y al honor también puede ofrecer protección a la memoria de los muertos.

Y por último, nada impide que un Estado miembro extienda el alcance de la normativa nacional que adapta el Derecho interno a la Directiva a situaciones que no están comprendidas en el ámbito de aplicación de esta última, siempre que ninguna otra norma de Derecho comunitario se oponga a ello, tal como ha recordado el Tribunal de Justicia de las Comunidades Europeas[16]. Es posible que algún legislador nacional decida ampliar las disposiciones de la legislación nacional sobre protección de datos a algunos aspectos referentes al tratamiento de los datos de personas fallecidas, cuando exista un interés legítimo que lo justifique[17].

Nasciturus

La medida en que las normas de protección de datos pueden aplicarse antes del nacimiento de una persona depende de la posición general de los ordenamientos jurídicos nacionales respecto a la protección del *nasciturus* (el concebido pero no nacido). Para tener en cuenta, principalmente, derechos de herencia, algunos Estados miembros consideran al *nasciturus* como nacido a efectos del reconocimiento de derechos (y, por lo tanto, puede recibir una herencia o aceptar una donación), a condición de que llegue a nacer. En otros Estados miembros, disposiciones legales particulares otorgan al *nasciturus* una protección específica, también sujeta a la misma condición. Para determinar si las normas nacionales de protección de datos cubren también la información sobre el *nasciturus*, debe tenerse en cuenta ese posicionamiento general del ordenamiento jurídico nacional junto con la idea de que la finalidad de las normas de protección de datos es proteger a las personas.

Una segunda cuestión es la que plantea la consideración de que la respuesta general del ordenamiento jurídico se basa en la premisa de que la situación de nasciturus se circunscribe temporalmente al período de embarazo. Esa reflexión no tiene en cuenta el hecho de que la situación puede en realidad prolongarse mucho más tiempo, como sucede en el caso de los embriones congelados. Por último, pueden encontrarse respuestas legales específicas en disposiciones particulares sobre técnicas de reproducción, en las que se aborda el uso de la información genética o médica sobre los embriones.

Personas jurídicas

Dado que la definición de datos personales hace referencia a las personas físicas, la información relativa a las personas jurídicas no está en principio cubierta por la Directiva[18]. Sin embargo, en algunas ocasiones, determinadas normas de protección de datos pueden aplicarse indirectamente a la información relativa a la actividad empresarial o las personas jurídicas.

---

16 Sentencia del Tribunal de Justicia de las Comunidades Europeas en el asunto C - 101/2001(Lindqvist) de 6.11.2003, apartado 98, Rec. 2003 p. I-12971.

17 Acta del Consejo de la Unión Europea, de 8.2.1995, documento 4730/95: «Ref artículo 2, a) *el Consejo y la Comisión confirman que compete a los Estados miembros establecer si y hasta qué punto esta Directiva se aplica a las personas fallecidas.*»

18 Considerando 24 de la Directiva: «*Considerando que las legislaciones relativas a la protección de las personas jurídicas respecto del tratamiento de los datos que las conciernan no son objeto de la presente Directiva*.».

Algunas disposiciones de la Directiva 2002/58/CE (Directiva sobre la privacidad y las comunicaciones electrónicas) se aplican también a las personas jurídicas. En su artículo 1, apartado 2, se establece que: «*Las disposiciones de la presente Directiva especifican y completan la Directiva 95/46/CE a los efectos mencionados en el apartado 1. Además, protegen los intereses legítimos de los abonados que sean personas jurídicas*». Por consiguiente, los artículos 12 y 13 amplían el ámbito de aplicación de algunas disposiciones referentes a las guías de abonados y a las comunicaciones no solicitadas a las personas jurídicas.

La información referente a personas jurídicas también puede ser considerada, en función de sus características, como información «sobre» personas físicas, de conformidad con los criterios establecidos en este documento. Así puede suceder cuando la denominación de la persona jurídica tiene su origen en el nombre de una persona física. Otro ejemplo puede ser el del correo electrónico de una empresa, utilizado normalmente por un empleado determinado o el de la información sobre una pequeña empresa (jurídicamente hablando un «objeto» más que una persona jurídica) que pueden describir el comportamiento de su usuario o propietario. En todos estos casos, en los que los criterios de «contenido», «finalidad» o «resultado» permiten considerar la información relativa a una persona jurídica o a actividades empresariales como información «sobre» una persona física, tal información debe ser calificada como datos personales, debiéndosele aplicar las normas de protección de datos.

El Tribunal de Justicia de las Comunidades Europeas ha dejado claro que nada impide que un Estado miembro extienda el alcance de la normativa nacional que adapta el Derecho interno a la Directiva a situaciones que no están comprendidas en el ámbito de aplicación de esta última, siempre que ninguna otra norma de Derecho comunitario se oponga a ello[19]. En consecuencia algunos Estados miembros como Italia, Austria o Luxemburgo han extendido el alcance de determinadas disposiciones de sus respectivos ordenamientos internos adoptadas de conformidad con la Directiva (como las relativas a las medidas de seguridad) al tratamiento de datos sobre personas jurídicas.

Como en el caso de la información sobre personas fallecidas, algunas adaptaciones de índole práctica introducidas por el responsable de los datos pueden hacer que los datos sobre una persona jurídica estén *de facto* sujetos a las normas de protección de datos. En los casos en que el responsable de los datos recoja datos sobre personas físicas y jurídicas indistintamente y los incluya en los mismos grupos de datos, el diseño de los mecanismos de tratamiento de los datos y el sistema de auditoría pueden concebirse para que cumplan las normas de protección de datos. De hecho, puede que al responsable le resulte más fácil aplicar las normas de protección de datos a todos los tipos de información contenidos en sus ficheros que intentar descifrar qué hace referencia a la persona física y qué a las personas jurídicas.

IV. ¿QUÉ SUCEDE SI LOS DATOS NO ENCAJAN DENTRO DE LA DEFINICIÓN?

Como se ha visto a lo largo de todo este documento, existen ocasiones en las que la información no puede ser considerada como datos personales. Así sucede, por ejemplo, cuando no puede afirmarse que los datos se refieren a una persona física, o cuando no

[19] Sentencia del Tribunal de Justicia de las Comunidades Europeas en el asunto C -101/2001(Lindqvist), de 6.11.2003, apartado 98, Rec. 2003 p. I-12971.

cabe hablar de persona identificada o identificable. Si la información que se está tratando no encaja en el concepto de «datos personales», la consecuencia es que la Directiva no se aplica, de conformidad con su artículo 3. No obstante, ello no significa que las personas puedan quedar totalmente desprotegidas en esos casos. Sobre este particular, hay que tener en cuenta las siguientes consideraciones.

Si la Directiva no se aplica, pueden entrar en juego las normas nacionales de protección de datos. De conformidad con lo establecido en su artículo 34, los destinatarios de la Directiva son los Estados miembros. Fuera del ámbito de aplicación de la Directiva, los Estados miembros no están sujetos a las obligaciones que ésta impone, básicamente, adoptar las disposiciones legales, reglamentarias y administrativas necesarias para darle cumplimiento. Sin embargo, como el Tribunal de Justicia de las Comunidades Europeas ha dejado claro, nada impide que un Estado miembro extienda el alcance de la normativa nacional que adapta el Derecho interno a la Directiva a situaciones que no están comprendidas en el ámbito de aplicación de esta última, siempre que ninguna otra norma de Derecho comunitario se oponga a ello. Por consiguiente, puede perfectamente suceder que determinadas situaciones en las que no se puede hablar de tratamiento de datos personales en el sentido de la Directiva, estén, sin embargo, sujetas a medidas protectoras con arreglo al Derecho nacional. Éste puede aplicarse, por ejemplo, a un tema como el de los datos cifrados, independientemente de que se trate de datos personales o no.

En aquellos casos en que las normas de protección de datos no se apliquen, determinadas actividades pueden, no obstante, infringir el artículo 8 del Convenio Europeo de Derechos Humanos y Libertades Fundamentales, que protege el derecho a la vida privada y familiar, de acuerdo con la jurisprudencia de mayor alcance del Tribunal Europeo de Derechos Humanos. Otros conjuntos de normas, como el Derecho de daños, el Derecho penal o las leyes contra la discriminación también pueden ofrecer protección a las personas físicas en los casos en que las normas de protección de datos no sean aplicables y estén en juego intereses legítimos.

V. CONCLUSIONES

En el presente Dictamen, el Grupo de trabajo ofrece una serie de orientaciones sobre cómo debe entenderse y aplicarse el concepto de datos personales de la Directiva 95/46/CE y de la legislación comunitaria adoptada en aplicación de la misma en diversas situaciones.

En términos generales se ha señalado que el legislador europeo se propuso adoptar un concepto amplio de datos personales, aunque ese concepto no es ilimitado. Nunca hay que olvidar que el objetivo de las disposiciones de la Directiva es proteger los derechos y libertades fundamentales individuales, en especial el derecho a la intimidad, en lo que se refiere al tratamiento de datos personales. Por ello, estas normas se concibieron para ser aplicadas en situaciones en las que los derechos individuales pueden correr peligro y, por tanto, necesitar protección. El ámbito de aplicación de las normas de protección de datos no debe llevarse a su extremo, pero también debe evitarse una limitación indebida del concepto de datos personales. La Directiva ha definido su ámbito de aplicación, excluyendo diversas actividades, y permite cierta flexibilidad al aplicar las normas a las actividades que entran en su ámbito de aplicación. Las autoridades de protección de datos desempeñan una misión fundamental en la búsqueda de una aplicación equilibrada de las mismas (véase el epígrafe II).

El análisis del Grupo de trabajo se ha basado en los cuatro «componentes» principales que pueden distinguirse en la definición de «datos personales», esto es: «toda información», «sobre», «identificada o identificable» y «persona física». Estos cuatro componentes están estrechamente ligados y se complementan entre sí, pero juntos determinan si una determinada información debe ser considerada como «datos personales». Este análisis se ilustra con ejemplos extraídos de las prácticas de las autoridades nacionales encargadas de la supervisión de la protección de datos.

- El primer componente - «toda información» - sugiere una interpretación lata del concepto, independientemente de la naturaleza o del contenido de la información y del soporte técnico en el que se presente. Esto significa que tanto la información objetiva como la subjetiva sobre una persona, cualquiera que sea su amplitud, y con independencia del soporte técnico que la contenga, puede considerarse como «datos personales». El dictamen también analiza la cuestión de los datos biométricos y su distinción jurídica con respecto a las muestras humanas de las que pueden extraerse (véase el epígrafe III.1).

- El segundo componente - «sobre» - no ha suscitado hasta ahora mucho interés, pero es crucial en la determinación del alcance sustantivo del concepto, especialmente en relación con objetos y nuevas tecnologías. El dictamen proporciona tres elementos alternativos - «contenido», «finalidad» o «resultado» - para determinar si la información versa «sobre» una persona física. Este componente abarca asimismo la información que puede tener claras repercusiones sobre la manera en que se trata o se valora a una persona (véase el epígrafe III.2).

- El tercer componente - «identificada o identificable» - se centra en las condiciones que deben darse para poder considerar a una persona como «identificable», y especialmente en «los medios que puedan ser razonablemente utilizados» por el responsable del tratamiento o por cualquier otra persona para identificar a dicha persona. El contexto y las circunstancias particulares de cada caso concreto tienen un papel importante en este análisis. El dictamen también trata la «*seudonimización*» y el uso de «datos cifrados» en la investigación estadística y farmacéutica (véase el epígrafe III.3).

- El cuarto componente - «persona física» – se centra en el requisito de que los «datos personales» se refieran a «seres vivos». El dictamen también analiza las conexiones con los datos sobre las personas fallecidas, el *nasciturus* y las personas jurídicas (véase el epígrafe III.4).

Por último, el dictamen se ocupa de lo que sucede si los datos no encajan en la definición de «datos personales». Para tratar de solucionar los posibles problemas que suscitan estos casos existen diferentes vías, incluido el recurso a la legislación nacional fuera del ámbito de aplicación de la Directiva, siempre que ninguna otra norma de Derecho comunitario se oponga a ello (véase el párrafo IV).

El Grupo de trabajo invita a todas las partes interesadas a estudiar cuidadosamente las orientaciones proporcionadas en este dictamen y a tenerlas en cuenta al interpretar y aplicar disposiciones del Derecho nacional para que se atengan a la Directiva 95/46/CE.

Los miembros del Grupo de trabajo, en su mayoría representantes de las autoridades nacionales de protección de datos, están firmemente decididos a desarrollar las orientaciones ofrecidas en el presente dictamen en sus respectivos ámbitos

jurisdiccionales, así como a garantizar una aplicación adecuada de sus legislaciones nacionales en sintonía con la Directiva 95/46/CE.

El Grupo de trabajo se propone aplicar y desarrollar las orientaciones del presente dictamen siempre que sea apropiado, así como tenerlas cuidadosamente en cuenta en sus trabajos posteriores, en particular al tratar temas como el de la gestión de la identidad en el contexto de los sistemas electrónicos al servicio de la administración pública y de la sanidad (e-Gobierno y sanidad en línea), así como en el de la RFID (identificación por radiofrecuencia). En cuanto a este último tema, el Grupo de trabajo tiene intención de contribuir a un futuro análisis sobre la manera en que las normas de protección de datos pueden incidir en el uso de la RFID y sobre la eventual necesidad de adoptar nuevas medidas para garantizar un respeto adecuado de los derechos de protección de datos y de los intereses presentes en ese contexto.

Por último, el Grupo de trabajo agradecería cualquier observación de las partes interesadas y de las autoridades de protección de datos sobre la aplicación práctica de las orientaciones del presente dictamen, incluido cualquier otro ejemplo distinto de los mencionados en este documento. El Grupo de trabajo tiene intención de abordar de nuevo este tema a su debido tiempo, con objeto de perfeccionar y consolidar la definición común del concepto clave de datos personales y asegurar una aplicación uniforme y una mejor ejecución de la Directiva 95/46/CE y de cualquier otra legislación comunitaria relacionada con ella.

Por el Grupo de protección

El Presidente
Peter SCHAAR