GRUPO DE PROTECCIÓN DE DATOS DEL ARTÍCULO 29

01197/11/ES
WP187

Dictamen 15/2011 sobre la definición del consentimiento

adoptado el 13 de julio de 2011

El Grupo se creó en virtud del artículo 29 de la Directiva 95/46/CE. Es un órgano consultivo europeo independiente en materia de protección de datos y derecho a la intimidad. Sus cometidos se describen en el artículo 30 de la Directiva 95/46/CE y en el artículo 15 de la Directiva 2002/58/CE.

De su secretaría se encarga la Dirección C (Derechos fundamentales y ciudadanía) de la Comisión Europea, Dirección General de Justicia, B-1049 Bruselas, Bélgica, despacho nº MO 59 02/013.

Sitio web: http://ec.europa.eu/justice/policies/privacy/index_es.htm

Resumen

El Dictamen analiza exhaustivamente el concepto de consentimiento tal como figura actualmente en la Directiva de protección de datos y en la Directiva sobre privacidad. A partir de la experiencia de los miembros del Grupo del artículo 29, recoge numerosos ejemplos de consentimiento válido e inválido, centrándose en elementos clave como el significado de los términos «manifestación», «libre», «específica», «inequívoca», «explícita», «informada», etc. El Dictamen también aclara algunos aspectos relacionados con el concepto de consentimiento. Por ejemplo, los plazos en que se debe obtener el consentimiento, cómo distinguir entre derecho de oposición y consentimiento, etc.

El consentimiento es uno de los fundamentos jurídicos del tratamiento de datos personales. Es un elemento importante que no excluye, según el contexto, la posibilidad de otros fundamentos jurídicos tal vez más adecuados desde el punto de vista del responsable del tratamiento y el interesado. Si se utiliza correctamente, el consentimiento es un instrumento que permite al interesado controlar el tratamiento de sus datos. Si se utiliza de forma incorrecta, el control por el interesado resulta ilusorio y el consentimiento deja de ser una base adecuada del tratamiento.

El presente Dictamen se dicta en parte como respuesta a una petición formulada por la Comisión en el marco de la actual revisión de la Directiva de protección de datos. Por tanto, contiene recomendaciones a considerar en dicha revisión. Entre estas figuran:

(i) la aclaración del significado del consentimiento «inequívoco» y la explicación de que sólo el consentimiento basado en manifestaciones o acciones que expresen conformidad constituye un consentimiento válido;

(ii) la exigencia a los responsables del tratamiento de que apliquen mecanismos para comprobar el consentimiento (en el marco de la obligación general de responsabilidad);

(iii) la introducción de un requisito específico relativo a la calidad y accesibilidad de la información, que constituyen la base del consentimiento, y

(iv) una serie de sugerencias sobre los menores y otras personas que carecen de capacidad jurídica.

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

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

Vistos 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

El consentimiento del interesado ha sido siempre un concepto clave de la protección de datos, sin que siempre esté claro cuando es necesario y cuales son las condiciones que deben cumplirse para que sea válido. Esto implica la posibilidad de diferentes enfoques y opiniones divergentes en cuanto a las buenas prácticas en los diferentes Estados miembros. La situación en que se encuentran los interesados puede debilitarse. El problema se ha agravado a medida que la actividad de tratamiento de datos personales ha ido adquiriendo una importancia creciente en la sociedad actual, tanto en entornos en línea como fuera de líneas, en los que a menudo participan diferentes Estados miembros. Por este motivo, el Grupo de trabajo del artículo 29, dentro de su programa de trabajo para 2010-2011, ha decidido examinar atentamente este asunto.

El consentimiento es también uno de los temas sobre los que la Comisión ha solicitado contribuciones en el contexto de la revisión de la Directiva 95/46/CE. La Comunicación de la Comisión sobre «Un enfoque global de la protección de los datos personales en la Unión Europea»[1] afirma lo siguiente: «La Comisión estudiará los medios de clarificar y reforzar las normas en materia de consentimiento». La Comunicación lo explica[2] como sigue:

«Cuando se exige un consentimiento informado, las normas vigentes prevén que el consentimiento de la persona sobre el tratamiento de sus datos personales debería ser una «manifestación de voluntad, libre, específica e informada» por la que acepta este tratamiento. Ahora bien, actualmente estas condiciones son objeto de distintas interpretaciones en los Estados miembros, desde la obligación general de obtener un consentimiento escrito a la aceptación de un consentimiento implícito.»

«Además, en el medio en línea - vista la opacidad de las políticas de confidencialidad - las personas tienen a menudo más dificultades para informarse de sus derechos y dar un consentimiento informado. Esto es tanto más complejo debido a que, en algunos casos, no está claro lo que constituye un consentimiento libre, específico e informado respecto del tratamiento de datos, como en el ámbito de la publicidad en línea basada en el

---

1 COM (2010) 609 final, de 4.11.2010.

2 El primer informe de la Comisión sobre la aplicación de la Directiva sobre protección de datos (95/46/CE) COM (2003) 265 final, declaraba lo siguiente en su página 17: «El concepto de "consentimiento inequívoco" [letra a) del artículo 7], en concreto, frente al concepto de "consentimiento explícito" del artículo 8, debe aclararse mejor e interpretarse de manera más uniforme. Es preciso que los agentes sepan en qué consiste un consentimiento válido en las situaciones concretas en línea.»

comportamiento, donde se considera a veces, pero no siempre, que los parámetros del navegador del internauta expresan su consentimiento.»

«Conviene pues clarificar las condiciones del consentimiento del interesado, con el fin de garantizar que se concede siempre con conocimiento de causa, y de garantizar que el interesado es plenamente consciente de que da su autorización y respecto a qué tratamiento, de conformidad con lo dispuesto en el artículo 8 de la Carta de los Derechos Fundamentales de la UE. La claridad de los conceptos clave puede también favorecer las iniciativas de autorregulación destinadas a desarrollar soluciones prácticas conformes al Derecho de la Unión.»

Para responder a la petición de la Comisión y aplicar su programa de trabajo 2010-2011, el Grupo del Artículo 29 se comprometió a elaborar un dictamen. El objetivo del dictamen es aclarar ciertas cuestiones a fin de que el marco legal existente sea entendido de forma uniforme. Al mismo tiempo, esta acción está en consonancia con anteriores dictámenes sobre otras disposiciones clave de la Directiva[3]. Los posibles cambios del marco existente tomarán su tiempo, por lo que clarificar el concepto actual de «consentimiento» y sus principales elementos es conveniente y beneficioso. La aclaración de las disposiciones existentes también contribuirá a poner de relieve los aspectos que requieren mejoras. Así, sobre la base del análisis, el Dictamen se propone formular recomendaciones estratégicas destinadas a la Comisión y los responsables políticos para que las tengan en cuenta al considerar los cambios del marco legal existente en materia de protección de datos.

El contenido básico del Dictamen es el siguiente: tras una presentación general de los antecedentes legislativos y la función del consentimiento en la normativa de protección de datos, se examinan los distintos elementos y requisitos de validez del consentimiento con arreglo a la normativa aplicable, incluidas algunas partes relevantes de la Directiva 2002/58/CE sobre privacidad. El análisis se ilustra con ejemplos prácticos basados en experiencias nacionales. Este ejercicio se basa en las recomendaciones recogidas en la parte final del presente Dictamen sobre la necesidad de introducir determinados elementos para la búsqueda y obtención del consentimiento válido con arreglo a la Directiva. También formula recomendaciones estratégicas destinadas a los responsables de las políticas para que las consideren en el contexto de la revisión de la Directiva 95/46/CE.

[3] Como el Dictamen 8/2010 sobre la ley aplicable, adoptado el 16.12.2010 (WP 179) y el Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento», adoptado el 16.2.2010 (WP 169).

II. Observaciones generales y aspectos de las políticas

II.1. Breve historial

Aunque algunas normativas de protección de datos/privacidad adoptadas en la década de 1970 consideraban el consentimiento como uno de los fundamentos jurídicos del tratamiento de datos personales[4], esto no se reflejó en el Convenio 108 del Consejo de Europa[5]. No hay ningún motivo aparente para que el Convenio no reconozca en mayor medida el papel del consentimiento[6].

En el ámbito de la UE, la referencia al consentimiento como criterio de legitimación de las operaciones de tratamiento de datos personales se previó desde el principio del proceso legislativo que culminó con la adopción de la Directiva 95/46/CE. El artículo 12 de la propuesta de la Comisión[7] de 1990 estableció las características que debe tener el consentimiento para legitimar las operaciones de tratamiento de datos: debe ser «otorgado expresamente» y «específico». El artículo 17, relativo a los datos sensibles, exigía que el consentimiento fuera «explícito y escrito». La propuesta modificada de la Comisión[8] de 1992 introdujo un texto parecido a la definición del «consentimiento del interesado» del actual artículo 2, letra g), al sustituir el artículo 12 original. Establecía que el consentimiento debía ser «libre y específico». La referencia a «otorgado expresamente» se sustituyó por el consentimiento como «indicación expresa de los deseos del interesado». La exposición de motivos que acompañaba a la propuesta modificada de 1992[9] declaraba que el consentimiento podía obtenerse verbalmente o por escrito. En cuanto a los datos sensibles, se mantuvo el requisito del consentimiento «escrito». En 1992, la propuesta modificada de la Comisión reorganizó la anterior propuesta e introdujo un artículo 7 que regula los fundamentos jurídicos del tratamiento. El artículo 7, letra a), señala que el tratamiento podrá realizarse «previo consentimiento del interesado»; La lista original incluía, como actualmente, cinco fundamentos jurídicos adicionales (además del consentimiento) que pueden utilizarse para legitimar el tratamiento de datos.

La posición común del Consejo[10] de 1995 adoptó la definición final (actual) del consentimiento. Se definió como «toda manifestación de voluntad, libre, específica e

---

[4] Véase por ejemplo el artículo 31 de la Ley francesa nº 78-17 *relative a l'informatique, aux fichiers et aux liberté*, de 6 de enero de 1987.

[5] Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (denominado «Convenio 108»). Entró en vigor el 1 de octubre de 1985.

[6] El Convenio 108 introdujo los conceptos de «tratamiento legal» y «finalidad legítima» (artículo 5) pero, a diferencia de la Directiva 95/46/CE no enumera los criterios del tratamiento de datos legítimo. El consentimiento del interesado sólo se reconoce en el contexto de la asistencia mutua (artículo 15). Sin embargo, el requisito del «consentimiento» ha sido mencionado reiteradamente en diversas recomendaciones posteriores del Comité de Ministros.

[7] Propuesta de Directiva relativa a la protección de las personas físicas en relación con el tratamiento de los datos personales, COM (90), 314 final, SYN 287 y 288, Bruselas, 13 de septiembre de 1990.

[8] Propuesta modificada de Directiva del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de los datos de carácter personal y a la libre circulación de estos datos, COM (92) 422 final- SYN 287, Bruselas, 15 de octubre de 1992.

[9] Véase la página 11 de la propuesta modificada de Directiva del Consejo 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, COM (92) final – SYN 287, Bruselas, 15 de octubre de 1992.

[10] Posición Común del Consejo sobre la propuesta de Directiva del Parlamento Europeo y del Consejo, 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, (00/287) COD, adoptada el 15.3.95.

informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan». El principal cambio con respecto a la posición de 1992 de la Comisión fue la supresión del término «expresa» que precedía al término «manifestación». Al mismo tiempo, se añadió el término «inequívoca» en el artículo 7, letra a), que quedó redactado como sigue: «si el interesado ha dado su consentimiento de forma inequívoca». El requisito de consentimiento escrito para los datos sensibles se sustituye por el «consentimiento explícito».

Las motivaciones del Consejo[11] no explicaban específicamente esos cambios. En la página 4 se señalaba, no obstante, que « ... numerosas modificaciones que … introducen una flexibilidad por la cual, a la vez que garantizan un nivel equivalente de protección …, no deberían conducir a una disminución del nivel de protección, porque permiten una aplicación eficaz y no burocrática de los principios generales establecidos en función de la gran variedad de … los tratamientos de datos de carácter personal.»

La función del consentimiento ha sido reconocida expresamente por la Carta de los Derechos Fundamentales de la UE en relación con la protección de datos personales. Su artículo 8, apartado 2, establece que los datos personales pueden ser tratados «sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley». Por lo tanto, el consentimiento se reconoce como un aspecto esencial del derecho fundamental a la protección de datos de carácter personal. Al mismo tiempo, el consentimiento según la Carta no es el único fundamento jurídico que permite tratar los datos personales; la Carta reconoce explícitamente que pueden establecerse por ley otros fundamentos legítimos, como es el caso de la Directiva 95/46/CE.

En resumen, los antecedentes legislativos, especialmente en la UE, muestran que el consentimiento ha desempeñado una función importante en la concepción de la protección de datos y la privacidad. También indican que el consentimiento no ha sido considerado el único fundamento jurídico de legitimación de las operaciones de tratamiento de datos. En el historial normativo de la Directiva 95/46/CE se pone de manifiesto el consenso sobre las condiciones del consentimiento válido, a saber: «[manifestación de voluntad] libre, específica e informada». Sin embargo, también muestra cierta incertidumbre sobre las formas de manifestación del consentimiento: explícito, escrito, etc. Este aspecto se analiza más adelante.

[11] Véase la página 4 de la Posición Común.

II.2. <u>Función del concepto: fundamento de legalidad</u>

Motivo general/específico:

En la Directiva, el consentimiento es tanto un criterio general de legalidad (artículo 7) como un fundamento específico en determinados contextos específicos [artículo 8, apartado 2, letra a), y artículo 26, apartado 1, letra a)]. El artículo 7 menciona el consentimiento como el primero de los seis elementos de legitimación del tratamiento de datos personales, mientras que el artículo 8 prevé la posibilidad de utilizar el consentimiento para legitimar un tratamiento de determinadas categorías de datos (sensibles) que de otro modo estaría prohibido. En este último caso, la norma para obtener el consentimiento es más exigente que la norma general, ya que el consentimiento debe ser «explícito».

Además, la Directiva permite la interacción con otras normativas, como se indica en el considerando 23: «Los Estados miembros están facultados para garantizar la protección de las personas tanto mediante una ley general relativa a la protección de las personas físicas en relación con el tratamiento de los datos de carácter personal como mediante leyes sectoriales». En la práctica, el funcionamiento de este sistema es complejo: los Estados miembros han adoptado su propio enfoque y en algunos casos se ha generado diversidad.

El concepto de consentimiento no siempre se ha adoptado literalmente a nivel nacional. Por ejemplo, el concepto general de consentimiento no está definido en la normativa francesa de protección de datos, aunque su significado ha sido explicado de forma coherente y precisa en la jurisprudencia de la autoridad de protección de datos (CNIL) con referencia a la definición recogida en la Directiva de protección de datos. En el Reino Unido, el concepto ha surgido en el Derecho consuetudinario por referencia al texto de la Directiva. Además, el consentimiento se ha definido en ocasiones explícitamente en sectores específicos como la privacidad, la administración electrónica o la salud en línea. Por tanto, el concepto que se ha adoptado en normativas específicas interactuará con el adoptado en la normativa de protección de datos.

El concepto de consentimiento también se utiliza en otros ámbitos del Derecho, especialmente en el Derecho contractual. En este contexto, para garantizar la validez de un contrato se tendrán en cuenta otros criterios distintos de los especificados en la Directiva, tales como la edad, la influencia indebida, etc. No existe contradicción sino solapamiento entre el ámbito del Derecho civil y el ámbito de aplicación de la Directiva: esta no aborda las condiciones generales de validez del consentimiento en el ámbito del Derecho civil, pero tampoco las excluye. Esto significa, por ejemplo, que para examinar la validez de un contrato en el marco del artículo 7, letra b), de la Directiva, habrá que tener en cuenta los requisitos de Derecho civil. Además de la aplicación de las condiciones generales de validez del consentimiento previstas en el Derecho civil, el consentimiento exigido en el artículo 7, letra a), también debe interpretarse teniendo en cuenta el artículo 2, letra h), de la Directiva.

Esta interacción con otras normativas no sólo es evidente en el ámbito nacional sino también en el europeo. Los elementos de la Directiva se han interpretado de forma similar en otros contextos, como muestra una sentencia del Tribunal de Justicia en materia de Derecho laboral[12]: el consentimiento se exige en caso de renuncia a un derecho social. El Tribunal ha interpretado el concepto de consentimiento con arreglo a la Directiva 93/104 relativa a determinados aspectos de la ordenación del tiempo de trabajo. El Tribunal declaró que el «acuerdo del trabajador» implicaba el consentimiento del trabajador (no del sindicato en nombre del trabajador), y consideró que «acuerdo» (…) significaba consentimiento libre y con conocimiento de causa. También mantuvo que el trabajador que firma un contrato de trabajo con referencia a un acuerdo colectivo que autoriza una ampliación del tiempo de trabajo no cumplía los requisitos de consentimiento libre y explícito, con pleno conocimiento de causa. Esta interpretación del consentimiento en un contexto específico es muy parecida a la definición de la Directiva 95/46/CE.

El consentimiento no es el único fundamento de legalidad

La Directiva presenta claramente el consentimiento como un fundamento de legalidad. Sin embargo, algunos Estados miembros lo consideran un fundamento preferente, en ocasiones parecido a un principio constitucional, vinculado al sistema de protección de datos como derecho fundamental. Otros Estados miembros lo consideran una de las seis opciones, un requisito operativo que no es más importantes que las otras opciones. La aclaración de la relación entre el consentimiento y los otros fundamentos de legalidad - por ejemplo, en relación con los contratos, las tareas de interés público o los intereses legítimos del responsable y el derecho de oposición - , contribuirá a poner de relieve la función del consentimiento en algunos casos específicos.

El orden en que se citan los fundamentos jurídicos en el artículo 7 es pertinente, pero no significa que el consentimiento sea siempre el fundamento más adecuado para legitimar el tratamiento de datos personales. El artículo 7 comienza con el consentimiento y pasa a enumerar los restantes fundamentos, incluidos los contratos y las obligaciones legales, hasta llegar gradualmente al equilibrio de intereses. Hay que señalar que los cinco fundamentos que siguen al consentimiento requieren una «prueba de necesidad» que limita estrictamente el contexto en el que se pueden aplicarse. Esto no significa que el requisito del consentimiento permita mayor margen de maniobra que otros fundamentos del artículo 7.

Además, la obtención del consentimiento no anula las obligaciones del responsable del tratamiento con arreglo al artículo 6 en lo que respecta a la imparcialidad, necesidad y proporcionalidad, así como a la calidad de los datos. Por ejemplo, incluso un tratamiento de datos personales basado en el consentimiento del usuario no legitimaría la recopilación excesiva de datos para un fin particular.

La obtención del consentimiento tampoco permite eludir otras disposiciones como el artículo 8, apartado 5. Sólo en circunstancias muy limitadas puede el consentimiento legitimar actividades de tratamiento de datos que de otro modo estarían prohibidas, especialmente en relación con el tratamiento de algunos datos sensibles (artículo 8), o permitir la utilización de datos personales para su posterior tratamiento, sea éste o no

[12] Sentencia del Tribunal de Justicia (Gran Sala) de 5 de octubre de 2004, Pfeiffer Roith, Süß, Winter, Nestvogel, Zeller, Döbele, en los asuntos acumulados C-397/01 a C-403/01.

compatible con la finalidad original. En principio, el consentimiento no debe considerarse una excepción a los otros principios de protección de datos, sino una salvaguardia. Es, principalmente, un fundamento de legalidad que no exime de la aplicación de otros principios.

La elección del fundamento jurídico más adecuado no siempre es evidente, especialmente entre las letras a) y b) del artículo 7. Según el artículo 7, letra b), el tratamiento deberá ser necesario para cumplir el contrato o para la adopción de medidas precontractuales a instancia del interesado, sin más condiciones. El responsable del tratamiento que utilice el artículo 7, letra b), como fundamento jurídico, en el contexto de la celebración de un contrato, no podrá prorrogarlo para justificar un tratamiento de datos que exceda de lo necesario: deberá justificar el tratamiento adicional mediante un consentimiento específico sujeto a los requisitos del artículo 7, letra a). Esto pone de manifiesto la necesidad de un mayor grado de detalle en las cláusulas contractuales. En la práctica, significa que puede ser necesario disponer del consentimiento como condición adicional para algunas partes del tratamiento. O bien el tratamiento es necesario para la ejecución del contrato, o bien deberá obtenerse el consentimiento (libre).

Algunas transacciones pueden basarse simultáneamente en una serie de fundamentos jurídicos. Es decir, cualquier tratamiento de datos deberá en todo momento conformarse a uno o más fundamentos jurídicos. No se excluye la aplicación simultánea de diversos fundamentos, siempre en el contexto adecuado. La recogida de datos y el tratamiento de datos personales pueden ser necesarios en virtud de un contrato con el interesado – artículo 7, letra b); otras operaciones de tratamiento pueden ser necesarias como consecuencia de una obligación jurídica - artículo 7, letra c); la recogida de información adicional pueden requerir un consentimiento inequívoco – artículo 7, letra a); y, por último, el tratamiento puede legitimarse por el equilibrio de intereses -artículo 7, letra f).

Ejemplo: compra de un automóvil
El responsable del tratamiento de datos puede estar autorizado para tratar datos personales con diversos fines y sobre la base de diversos fundamentos:
- datos necesarios para la compra del automóvil: artículo 7, letra b),
- para tramitar los documentos del vehículo: artículo 7, letra c),
- para los servicios de gestión de clientes (por ejemplo, para que el automóvil esté disponible en diferentes empresas filiales dentro de la UE): artículo 7, letra f),
- para transferir los datos a terceros para sus propias actividades de comercialización: artículo 7, letra a).

II.3. <u>Conceptos relacionados</u>

Control

Por lo general, el concepto de consentimiento está vinculado a la idea de que el interesado debe controlar el uso que se hace de sus datos. Desde la perspectiva de los derechos fundamentales, el control ejercido a través del consentimiento es un concepto importante. Al mismo tiempo y desde el mismo punto de vista, la decisión por la que una persona acepta una operación de tratamiento de datos debe estar sujeta a requisitos estrictos, teniendo en cuenta que dicha decisión puede implicar la renuncia a un derecho fundamental.

Aunque el consentimiento también influye a la hora de otorgar el control a los interesados, no es el único medio para conseguirlo. La Directiva prevé otros medios de control, en particular el derecho de oposición, pero éste constituye un instrumento diferente que debe ejercerse en otra fase del tratamiento, una vez que el tratamiento ha comenzado, y tiene un fundamento jurídico diferente.

El consentimiento está relacionado con el concepto de autodeterminación. La autonomía del interesado es a la vez una condición previa y una consecuencia del consentimiento: permite al interesado influir sobre el tratamiento de los datos. Sin embargo, como se expone en el próximo capítulo, este principio tiene límites y existen casos en que el interesado no está en condiciones de adoptar una auténtica decisión. El responsable del tratamiento de datos puede utilizar el consentimiento del interesado para transferir su responsabilidad a la persona. Por ejemplo, al autorizar la publicación de datos personales en Internet o su transferencia a una entidad dudosa en un tercer país, el interesado puede sufrir daños y el responsable del tratamiento sostener que aquel dio su consentimiento. Por consiguiente, es importante recordar que un consentimiento plenamente válido no exime al responsable del tratamiento de sus obligaciones, y no legitima un tratamiento que de otra forma sería injusto según el artículo 6 de la Directiva.

El concepto de control también está relacionado con el hecho de que el interesado puede retirar su consentimiento. La retirada no tiene carácter retroactivo, pero en principio debería evitar cualquier tratamiento posterior de los datos del interesado por el responsable del tratamiento. Más adelante se examina cómo se produce en la práctica la retirada (capítulo III).

Transparencia

Un segundo aspecto del consentimiento se refiere a la información: la transparencia con respecto al interesado. La transparencia es una condición para la posesión del control y de validez del consentimiento. La transparencia por si misma no es suficiente para legitimar el tratamiento de datos personales, pero es una condición esencial para garantizar la validez del consentimiento.

Para ser válido, el consentimiento debe estar informado. Esto implica que toda la información necesaria debe suministrarse en el momento en que se solicita el consentimiento, y que éste debe abordar los aspectos sustantivos del tratamiento que el consentimiento se propone legitimar. En principio, debe abarcar las informaciones enumeradas en el artículo 10 de la Directiva, pero también depende del momento y las circunstancias en que se solicite el consentimiento.

Con independencia de si se otorga o no el consentimiento, la transparencia del tratamiento de datos también es una condición de equidad que sigue siendo válida por si misma incluso después del momento de transmisión inicial de la información.

Actividad/plazos: formas de manifestación del consentimiento

Esta tercera dimensión se refiere a la forma en que se ejerce el control: ¿cómo puede expresarse el consentimiento y en qué momento debería solicitarse para garantizar que es auténtico? Estas preguntas tienen un impacto decisivo en la forma en que se ejerce e interpreta el consentimiento.

Aunque el plazo para solicitar el consentimiento no está especificado en la Directiva, del texto de diversas disposiciones se deduce claramente que, por regla general, el consentimiento debe otorgarse antes del comienzo del tratamiento[13]. La obtención del consentimiento antes del comienzo del tratamiento de datos constituye una condición fundamental para legitimar el tratamiento de datos. Este punto se desarrolla en el capítulo III.B en relación con la Directiva sobre privacidad.

El consentimiento, considerado como la autorización por la que la persona permite el tratamiento de datos que le conciernen, puede expresarse de distintas maneras: el artículo 2, letra h), se refiere a «manifestación»; debe ser inequívoco (artículo 7 *bis*) y explícito en cuanto a los datos sensibles (antiguo artículo 8). Ahora bien, es importante subrayar que el consentimiento es diferente del derecho de oposición previsto en el artículo 14. Mientras que en el artículo 7, letra a), el responsable del tratamiento no puede tratar los datos hasta la obtención del consentimiento del interesado, en el artículo 7, letra f), el responsable del tratamiento puede tratar los datos, con sujeción a condiciones y salvaguardias, mientras el interesado no se oponga. Tal como se recoge en el documento 114 del Grupo de trabajo: «Por tratarse de un acto positivo, la importancia del consentimiento excluye *de facto* cualquier sistema por el que el interesado sólo tendría derecho a oponerse a la transferencia después de haberse producido»[14].

Por estas razones, el derecho de oposición del antiguo artículo 14 de la Directiva no debe confundirse con el consentimiento. Este último es el fundamento jurídico del tratamiento de datos personales previsto en el antiguo artículo 7, letra a), el artículo 8, apartado 2, letra a), el artículo 26, apartado 1, y en diversas disposiciones de la Directiva 2002/58/CE.

II.4. Uso adecuado del consentimiento como base jurídica

Es necesario señalar que el consentimiento no es siempre el primer medio o el más deseable para legitimar el tratamiento de datos personales.

Algunas veces el consentimiento constituye una débil base para justificar el tratamiento de datos personales y pierde valor si se amplía o ajusta para adaptarlo a situaciones en las que nunca debería utilizarse. Es fundamental utilizar el consentimiento «en el contexto adecuado». Si se utiliza en circunstancias inadecuadas, debido a que los elementos que le confieren validez pueden faltar, se puede producir una situación de

[13] Por ejemplo, la versión alemana de la Directiva (y la Ley federal alemana de protección de datos) utilizan el concepto de *Einwilligung*. Este concepto se define en el Código civil alemán como «aceptación previa».

[14] Documento de trabajo (WP114) del Grupo del Artículo 29 sobre una interpretación común del artículo 26, apartado 1, de la Directiva 95/46/CE de 24 de octubre de 1995.

gran vulnerabilidad y, en la práctica, la posición de los interesados puede resultar *debilitada.*

Este enfoque ha sido ya respaldado por el Grupo de trabajo y el SEPD (Supervisor europeo de protección de datos) en sus aportaciones a los debates sobre el nuevo marco de protección de datos. Se ha afirmado, en particular, que « …no siempre es fácil determinar qué constituye un consentimiento verdadero e inequívoco. Determinados responsables del tratamiento de datos explotan esta incertidumbre recurriendo a métodos que excluyen toda posibilidad de dar un consentimiento verdadero e inequívoco» [15] contraviniendo las condiciones establecidas en el artículo 6 de la Directiva. En la misma línea, el WP29 ha observado que «la complejidad de las prácticas de recogida de datos, modelos empresariales, relaciones con los vendedores y aplicaciones tecnológicas llega en muchos casos a sobrepasar la capacidad o la voluntad de la persona para tomar decisiones de control sobre el uso e intercambio de información por medio de una elección activa»[16].

Es importante, por tanto, aclarar los límites de consentimiento y asegurarse de que sólo el consentimiento que se interprete conforme a la ley será considerado como tal[17].

III. <u>Análisis de las disposiciones</u>

El capítulo III A se centra en el análisis de la Directiva 95/46/CE. Algunas partes pertinentes de la Directiva 2002/58/CE sobre privacidad se analizan en el capítulo III.B. Se señala que las Directivas no son mutuamente excluyentes. Las condiciones generales de validez del consentimiento, según se establecen en la Directiva 95/46/CE, se aplican tanto en línea como en contextos fuera de línea. La Directiva 2002/58/CE especifica estas condiciones para algunos servicios en línea explícitamente identificados, siempre a la luz de las condiciones generales de la Directiva de protección de datos.

III.A <u>Directiva 95/46/CE</u>

El concepto de «consentimiento del interesado» se define en el artículo 2, letra h), y se utiliza posteriormente en los artículos 7, 8 y 26. La función del consentimiento también se menciona en los considerandos 30 y 45. Estas disposiciones y todos los detalles pertinentes se examinarán por separado y en el presente capítulo.

III.A.1. <u>Artículo 2, letra h)</u>

Con arreglo al artículo 2, letra h), el «consentimiento del interesado» significa: «toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan.» Esta definición contiene diferentes elementos clave que se analizan a continuación.

[15] Dictamen del Supervisor Europeo de Protección de datos, de 14 de enero de 2011, sobre la Comunicación de la Comisión sobre «Un enfoque global sobre la protección de los datos personales en la Unión Europea».

[16] «El futuro de la privacidad: contribución común a la consulta de la Comisión Europea sobre el marco jurídico para el derecho fundamental a la protección de los datos de carácter personal», 1 de diciembre de 2009, WP 168.

[17] Dictamen del Supervisor Europeo de Protección de datos, de 14 de enero de 2011, op.cit.

«… toda … manifestación de voluntad …mediante la que … ”

En principio, no hay límites a la forma que puede adoptar el consentimiento. Sin embargo, para ser válido con arreglo a la Directiva, debe haber una manifestación de voluntad. Aunque puede tratarse de «toda» manifestación, debe quedar claro cuáles son exactamente las formas que entran en la definición de manifestación.

La forma de manifestación (es decir, el modo en que se expresa la voluntad) no se define en la Directiva. Por razones de flexibilidad, el consentimiento «escrito» no figura en el texto final. Hay que subrayar que la Directiva se refiere a «toda» manifestación de voluntad. Esto abre la posibilidad de una interpretación amplia del alcance de dicha manifestación. La expresión mínima de manifestación podría ser cualquier tipo de señal, suficientemente clara para poder indicar la voluntad del interesado y comprensible por el responsable del tratamiento de datos. Los términos «manifestación» y «mediante la que» apuntan a una acción realmente necesaria (frente a una situación en que el consentimiento podría deducirse de la falta de acción).

El consentimiento debe incluir toda manifestación de voluntad *mediante la que* el interesado consienta: podría tratarse de una firma manuscrita en la parte inferior de un formulario de papel, pero también de declaraciones orales mediante las que el interesado consienta, o de un comportamiento del que pueda deducirse razonablemente el consentimiento. Más allá del ejemplo clásico de la firma, una tarjeta de visita introducida en un recipiente de vidrio podría entrar, por tanto, en la definición. Lo mismo se aplica si un individuo envía su nombre y dirección a una organización para obtener información de ella. En este caso, debe entenderse que su acción contribuye al tratamiento de dichos datos, en la medida en que es necesario tramitar y responder a su solicitud.

En su dictamen sobre la utilización de datos de localización para la prestación de servicios de valor añadido (WP115), el Grupo de trabajo examinó lo que habría que hacer para que las personas estén en condiciones de autorizar los servicios que requieren su localización automática (por ejemplo, la posibilidad de llamar a un número específico para obtener información sobre las condiciones meteorológicas en su lugar de localización). En ese caso, se reconoció que, si el usuario recibe de antemano información completa sobre el tratamiento de sus datos de localización, el hecho de llamar al número en cuestión equivaldría a consentir ser localizado.

Ejemplo: Paneles publicitarios de *Bluetooth*

Un instrumento publicitario en expansión consiste en paneles que envían mensajes en los que se pide que se establezca una conexión *Bluetooth* para enviar anuncios a las personas que pasan por las inmediaciones. Los mensajes se envían a las personas que tienen activados los mecanismos *Bluetooth* en el móvil. La mera activación de la función *Bluetooth* no constituye un consentimiento válido (ya que *Bluetooth* puede activarse para otros fines). Por otra parte, cuando alguien está informado de este servicio y se aproxima a pocos centímetros del panel con el móvil, se produce, por lo general, una manifestación de voluntad: así se comprueba cuáles son las personas realmente interesadas en recibir los anuncios. Se considera que únicamente estas personas han manifestado su consentimiento, y sólo ellas deben recibir los mensajes por teléfono.

Es dudoso que la falta de actuación - o quizás mejor, el comportamiento pasivo - también pueda interpretarse como una manifestación de voluntad en circunstancias muy concretas (es decir, en un contexto totalmente inequívoco). El concepto de «manifestación» es amplio, pero parece implicar una necesidad de acción. Otros elementos de la definición de consentimiento, y el requisito adicional del artículo 7, letra a), sobre el consentimiento inequívoco, avalan esta interpretación. El requisito de que el interesado debe manifestar su consentimiento parece indicar que la simple inacción es insuficiente y se requiere algún tipo de acción para crear el consentimiento, aunque sean posibles diferentes tipos de acciones que se evaluarán «según el contexto».

En la práctica, la falta de comportamiento activo del interesado planteará un problema al responsable del tratamiento a la hora de comprobar si el silencio significa aceptación o consentimiento. Por ejemplo, el responsable del tratamiento puede no tener la certeza necesaria de que existe consentimiento en el caso siguiente: imaginemos una situación en la que tras el envío de una carta a los clientes informándoles de una propuesta de transferencia de sus datos, salvo objeción por su parte en el plazo de dos semanas, sólo el 10% de los clientes responde. En este ejemplo, es discutible que el 90% que no respondió efectivamente esté de acuerdo con la transferencia. En tales casos, el responsable del tratamiento de datos no tiene ninguna indicación clara de la intención de los interesados. Además, no dispondrá de ningún indicio y, en consecuencia, no podrá demostrar que ha obtenido el consentimiento. En la práctica, la ambigüedad de una respuesta pasiva dificultará el cumplimiento de los requisitos de la Directiva.

« [manifestación] …libre, …»

El consentimiento únicamente puede ser válido si el interesado puede elegir una opción real y no hay ningún riesgo de engaño, intimidación, coerción o consecuencias negativas significativas en caso de que no consienta. Si las consecuencias del consentimiento socavan la libertad de elección de la persona, el consentimiento no es libre. La propia Directiva prevé en su artículo 8, apartado 2, letra a), que, en algunos casos, a determinar por los Estados miembros, la prohibición del tratamiento de categorías especiales de datos personales no puede ser suprimida por el consentimiento del interesado.

Un ejemplo de lo anterior es el caso del interesado que está bajo la influencia del responsable del tratamiento, como sucede en la relación laboral. En este ejemplo, aunque no necesariamente en todos los casos, el interesado puede estar en una situación de dependencia del responsable del tratamiento debido a la naturaleza de la relación o a circunstancias particulares, y puede temer recibir un trato diferente si no da su consentimiento para el tratamiento de los datos.

En varios dictámenes, el Grupo de trabajo ha estudiado los límites del consentimiento en situaciones en las que no puede manifestarse libremente. Se trata de sus dictámenes sobre los registros sanitarios electrónicos (WP131), el tratamiento de datos en el contexto del empleo (WP48) y el tratamiento de los datos por la Agencia Mundial Antidopaje (WP162).

En el documento WP131, el Grupo de trabajo afirmaba que «el consentimiento “libre” supone una decisión voluntaria, de un individuo en posesión de todas sus facultades, tomada sin ningún tipo de coacción, ya sea social, financiera, psicológica u otra.» El consentimiento dado bajo amenaza de no tratamiento o de tratamiento de menor calidad en una circunstancia médica no puede considerarse «libre». Cuando como consecuencia necesaria e inevitable de la circunstancia médica un profesional de la salud tenga que tratar datos personales en un sistema de HME, es equívoco que este profesional intente legitimar este tratamiento a través del consentimiento. El recurso al consentimiento debe limitarse a los casos en que el interesado tenga una auténtica libertad de elección y por tanto sea posteriormente capaz de retirar el consentimiento sin sufrir perjuicio alguno». [18]

Si, una vez retirado el consentimiento, el tratamiento de datos continúa sobre la base de otro fundamento jurídico, podrían surgir dudas sobre la utilización original del consentimiento como fundamento jurídico inicial: si el tratamiento se hubiera podido realizar desde el principio sobre la base de este otro fundamento, someter a la persona a una situación en la que se le pide que dé su consentimiento al tratamiento podría considerarse engañosa o intrínsecamente desleal. Otra cosa sería que cambiaran las circunstancias, por ejemplo si surgiera una nueva base jurídica en el curso del tratamiento, como una nueva ley reguladora de la base de datos en cuestión. Si este nuevo fundamento puede aplicarse válidamente al tratamiento, éste puede proseguir. Pero en la práctica estas circunstancias no son frecuentes. En principio, el consentimiento puede considerarse insuficiente si no se permite su retirada efectiva.

El Grupo de Trabajo ha adoptado una posición coherente sobre la interpretación del libre consentimiento en el contexto laboral[19]: «Cuando se requiera el consentimiento de un trabajador y exista un perjuicio potencial o real relevante derivado de la falta de consentimiento, se considerará que el consentimiento no cumple lo establecido en el artículo 7 o en el artículo 8 si no es otorgado libremente. Si no es posible para el trabajador denegarlo, no se considerará consentimiento. (…) Un ámbito conflictivo se presenta cuando otorgar el consentimiento es una condición para el empleo. En teoría, el trabajador puede denegar su consentimiento, pero la consecuencia podría ser la pérdida de una oportunidad de empleo. En tales circunstancias el consentimiento no se otorga libremente y por tanto no es válido. La situación está aún más clara cuando, como suele ser el caso, todos los empleadores imponen unas condiciones laborales iguales o similares.»

Ejemplo: fotos en Intranet

El consentimiento en el contexto laboral puede ser válido como muestra el siguiente ejemplo: una empresa decide crear una Intranet en la que figuren los nombres y funciones principales de los empleados. Se pregunta a cada uno de ellos si desea que su foto aparezca junto al nombre. Las personas que lo desean deben enviar una foto a una determinada dirección. Una vez recibida la información adecuada, la acción de enviar la foto equivale al consentimiento de la persona. Si la empresa posee fotos digitales de cada uno de los empleados y les solicita individualmente su consentimiento para descargarlas para los fines mencionados, se considera que el empleado que pulse el botón para dar el consentimiento está dando así su

[18] El documento WP162 sobre la AMA llega a la misma conclusión: «Las sanciones y consecuencias previstas en caso de eventual negativa de los participantes a cumplir las obligaciones del Código (por ejemplo, facilitar comunicación de datos de localización) han llevado al Grupo de Protección a considerar que el consentimiento no se daría libremente en ningún caso».

[19] Documento WP48 sobre el tratamiento de datos personales en el contexto laboral. El documento de trabajo WP114 del Grupo del artículo 29 sobre una interpretación común del artículo 26, apartado 1, de la Directiva 95/46/CE de 24 de octubre de 1995, también viene aquí al caso.

consentimiento válido. En cualquier caso, se respeta plenamente la decisión de los empleados en cuanto a la publicación de sus fotos en Intranet.

El contexto laboral exige un debate específico: los aspectos sociales y culturales de la relación laboral han de tenerse en cuenta, al igual que la interacción de los principios de protección de datos con otras normativas. En el contexto laboral, los datos de carácter personal pueden ser tratados para fines diversos:

- datos necesarios para el desempeño de las funciones del empleado: aplicación del artículo 7, letra b) – tratamiento necesario para la ejecución de un contrato;
- para determinar el derecho de los empleados a suscribir opciones sobre acciones: bien sobre la base del consentimiento, - artículo 7, letra a), o por su consideración de inherente a los aspectos administrativos de la relación laboral - artículo 7, letra b);
- tratamiento del número de afiliación a la seguridad social para fines de la seguridad social: artículo 7, letra c) – cumplimiento de una obligación jurídica o, en su caso, el artículo 8, letra b), - obligaciones en materia de Derecho laboral;
- tratamiento de datos étnicos: en algunos países, esto podría ser también una obligación de Derecho laboral - artículo 8, letra b), mientras que en otros países estaría estrictamente prohibido.

Aunque hay motivos de peso para suponer que el consentimiento es débil en estos contextos, su utilización no se excluye completamente en los casos en que existan garantías suficientes de que es realmente libre.

Con frecuencia, la relación de subordinación es la razón principal que impide que el consentimiento sea libre, pero otros elementos del contexto pueden influir también en la decisión del interesado. Puede tratarse, por ejemplo, de cuestiones financieras, emocionales o prácticas. El hecho de que la recogida de datos la realice una autoridad pública también puede influir de alguna manera en el interesado. Pero es difícil trazar la línea entre un simple estímulo y algo que ejerce una influencia real en la libertad de elección del interesado. Los ejemplos siguientes ilustran la naturaleza del esfuerzo o los costes para la persona que podrían influir en su decisión.

Ejemplo: historiales médicos electrónicos

En muchos Estados miembros se tiende a elaborar un resumen electrónico de los historiales médicos de los pacientes. Esto permite a los profesionales de la atención sanitaria acceder a datos clave cada vez que el paciente necesita tratamiento.

- En la primera hipótesis, la creación de un historial resumido es totalmente voluntaria y el paciente recibirá tratamiento con independencia de que haya dado o no su consentimiento para su creación. En este caso, el consentimiento para la elaboración del historial resumido se da libremente porque el paciente no resulta perjudicado por negar o retirar su consentimiento.

En la segunda hipótesis, existe un incentivo financiero moderado para elegir el historial médico electrónico. Los pacientes que rechazan el historial electrónico no sufren ninguna desventaja porque los costes no varían para ellos. También podría considerarse en este caso que son libres de consentir o no el nuevo sistema.

- En la tercera hipótesis, los pacientes que rechazan el sistema electrónico tienen que pagar un coste adicional considerable a la tarifa existente y el tratamiento de sus informes se retrasa considerablemente. Ello implica una clara desventaja para aquellos que no consienten, dado el propósito de incluir a todos ciudadanos en el sistema de salud en línea en una fecha programada. Por tanto, el consentimiento no es suficientemente libre. Habría que considerar, en consecuencia, la existencia de otros fundamentos legítimos para el tratamiento de datos personales o examinar la aplicación del artículo 8, apartado 3, de la Directiva 95/46/CE.

Ejemplo: escáneres de personas

La utilización de escáneres de personas se está generalizando en algunos espacios públicos, especialmente para acceder a la zona de embarque de los aeropuertos. Dado que los datos de los pasajeros se tratan en el momento en que tiene lugar el control[20], el tratamiento debe cumplir alguno de los fundamentos jurídicos previstos en el artículo 7. Atravesar los escáneres corporales se presenta a veces como una opción para los pasajeros, lo cual implica que el tratamiento podría justificarse por su consentimiento. Pero la negativa a atravesar los escáneres corporales pueden crear sospechas o dar lugar a controles adicionales como el cacheo. Muchos pasajeros consienten en ser escaneados porque así evitan posibles problemas o retrasos, dado que su prioridad es embarcar a bordo del vuelo a tiempo. Este tipo de consentimiento no es suficientemente libre. Dado que debe demostrarse la necesidad del tratamiento (por motivos de seguridad pública), su fundamento legítimo no reside en el artículo 7, letra a), sino en un acto del legislador (artículo 7, letras c) o e), del que se deriva la obligación que tienen los pasajeros de cooperar. Por lo tanto, la base del escáner corporal debe residir en la legislación. Esta también podría prever la elección por la persona entre el escáner y el control manual, pero sólo con carácter complementario y como medida adicional.

La naturaleza del responsable del tratamiento también puede ser decisiva a la hora de determinar el fundamento jurídico del tratamiento de datos personales. Es el caso de los responsables del tratamiento del sector público, donde el tratamiento de datos suele estar vinculado al cumplimiento de una obligación jurídica en el sentido del artículo 7, letra c), o al cumplimiento de una misión de interés público en el sentido del artículo 7, letra e). Por consiguiente, la utilización del consentimiento de la persona interesada para legitimar el tratamiento de datos no constituye una base jurídica adecuada. Esto es especialmente evidente en el tratamiento de datos personales por parte de autoridades públicas con poderes coercitivos tales como los servicios de seguridad, que actúan en el ámbito de su competencia al realizar actividades policiales y judiciales. Las autoridades policiales no puede basarse en el consentimiento de la persona para medidas que no están previstas o que de otro modo la ley no permitiría.

[20] Véase la carta de 11 de febrero de 2009 del Presidente del Grupo de Trabajo del Artículo 29 al Sr. D. Daniel Calleja Crespo, Director responsable de escáneres de personas en la DG TREN, en respuesta a la consulta de la Comisión sobre «El impacto de la utilización de escáneres en el ámbito de la seguridad de la aviación sobre los derechos humanos, la vida privada, la dignidad personal, la salud y la protección de datos». Disponible en http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2009-others_en.htm.

Es preciso reconocer, sin embargo, que aunque los Estados pueden tener la obligación legal de tratar datos personales, la persona no siempre tienen el deber de colaborar. Puede haber casos en que se presten servicios de «valor añadido» a los interesados, que pueden decidir utilizarlos o no. Pero en la mayoría de los casos el tratamiento es realmente obligatorio. A menudo no es fácil determinar si el tratamiento de datos personales por parte de las autoridades públicas se basa verdaderamente en el consentimiento de la persona. Con frecuencia, en el tratamiento de datos personales en el sector público se mezclan regímenes diversos, lo que puede generar incertidumbre y abusos si no está debidamente justificado por el consentimiento.

Si bien el consentimiento, en casos excepcionales, puede ser un motivo válido de tratamiento de datos personales por los Estados, debería realizarse un control cuidadoso en cada caso para saber si ha sido suficientemente libre. Como muestran los siguientes ejemplos, cuando el responsable del tratamiento es una autoridad pública, el fundamento jurídico para legitimar el tratamiento será el cumplimiento de una obligación jurídica con arreglo al antiguo artículo 7, letra c), o el cumplimiento de una misión de interés público con arreglo al antiguo artículo 7, letra e), en lugar del consentimiento.

Ejemplo: la administración electrónica
Los Estados miembros están desarrollando nuevas tarjetas de identidad con funcionalidades electrónicas en un *chip*. La activación de los servicios electrónicos de la tarjeta probablemente no será obligatoria. Pero sin activación, el usuario podría quedarse sin acceder a ciertos servicios administrativos que de otro modo serían de muy difícil acceso (transferencia de algunos servicios en línea, reducción de las horas de apertura). El consentimiento no puede considerarse un fundamento legítimo para justificar el tratamiento. En este caso, la ley reguladora del desarrollo de los servicios electrónicos, junto con todas las garantías adecuadas, debe ser el fundamento aplicable.

Ejemplo: datos PNR
Se ha debatido la cuestión de si el consentimiento de los pasajeros puede ser utilizado válidamente para legitimar la transferencia de datos de reservas (datos PNR) de las compañías aéreas europeas a las autoridades de los EE.UU. El Grupo de trabajo considera que el consentimiento de los pasajeros no se da libremente porque las compañías aéreas están obligadas a enviar los datos antes de la salida del vuelo y los pasajeros que desean volar no tienen, por consiguiente, ninguna otra alternativa real[21]. La base jurídica no es el consentimiento del pasajero, sino más bien, de conformidad con el artículo 7, letra c), las obligaciones previstas en el Acuerdo internacional entre la UE y los Estados Unidos sobre el tratamiento y la transferencia de los registros de nombres de los pasajeros (*Passenger Name Record*, PNR).

[21] Véase el Dictamen 6/2002 del Grupo de Trabajo del artículo 29 sobre la transmisión de listas de pasajeros y otros datos de las compañías aéreas a los Estados Unidos.

Ejemplo: censo nacional
Al elaborar el censo nacional se pide a la población que responda a diversas preguntas sobre su situación personal y profesional.
Es obligatorio responder a las preguntas. Además, el censo también incluye una pregunta cuya respuesta se indica claramente como facultativa y se refiere a los medios de transporte utilizados por los particulares. No existe ciertamente el libre consentimiento respecto de la parte principal del censo, pero puede elegirse libremente contestar o no a esta última pregunta facultativa. No obstante, no hay que olvidar que el objetivo principal que persigue el Estado al publicar el cuestionario es obtener respuestas. En general, el consentimiento no constituyen un fundamento válido en este contexto.

« [manifestación de voluntad]…específica…»

Para ser válido, el consentimiento debe ser específico. En otras palabras, el consentimiento indiscriminado sin especificar la finalidad exacta del tratamiento no es admisible.

Para ser específico, el consentimiento debe ser comprensible: referirse de manera clara y precisa al alcance y las consecuencias del tratamiento de datos. No puede referirse a un conjunto indefinido de actividades de tratamiento. Esto significa, en otras palabras, que el consentimiento se aplica en un contexto limitado.

El consentimiento debe darse en relación con los diversos aspectos del tratamiento, claramente identificados. Esto implica saber cuales son los datos y los motivos del tratamiento. Este conocimiento debería basarse en las expectativas razonables de las partes. Por tanto, el «consentimiento específico» está intrínsecamente relacionado con el hecho de que el consentimiento debe estar informado. Existe un requisito de precisión del consentimiento con respecto a los diferentes elementos del tratamiento de datos: no puede pretenderse que abarque «todos los fines legítimos» perseguidos por el responsable del tratamiento. El consentimiento debe referirse al tratamiento que es razonable y necesario en relación con la finalidad.

En principio, a los responsables del tratamiento les debería bastar con obtener el consentimiento una sola vez para las diferentes operaciones, siempre que estas entren dentro de las expectativas razonables del interesado.

Recientemente, el TJCE ha dictado una decisión prejudicial[22] en relación con el artículo 12, apartado 2, de la Directiva sobre privacidad, en la que se pronuncia sobre la necesidad de renovar el consentimiento de los abonados que ya han accedido a la publicación de sus datos personales en una guía, a fin de transferir sus datos personales para ser publicados por otros servicios de guía de usuarios. El Tribunal sostuvo que,

[22] Sentencia del Tribunal de 5 de mayo de 2011, *Deutsche Telekom AG* (asunto C - 543/09). Este caso empezó con la remisión formulada por el Tribunal Administrativo Federal de Alemania en relación con las guías de telecomunicaciones y, en particular, la interpretación del artículo 25, apartado 2, de la Directiva de servicio universal (2002/22/CE), y del artículo 12, apartado 2, de la Directiva sobre la privacidad (2002/58/CE). Está claramente relacionada con la función especial de las guías en la Directiva de servicio universal.

cuando el abonado haya sido correctamente informado de la posibilidad de que sus datos personales sean transmitidos a una tercera empresa y haya accedido a la publicación de dichos datos en una guía, no será necesario renovar el consentimiento del abonado para la transferencia de los datos, «siempre que se garantice que los datos no puedan utilizarse con otros fines más que aquéllos para los que se hayan recogido para su primera publicación» (apartado 65).

Ahora bien, puede requerirse un consentimiento diferenciado si el responsable se propone tratar los datos para fines diferentes. Por ejemplo, el consentimiento podría darse con respecto a la información sobre nuevos productos dirigida a la persona y con respecto a acciones de promoción específicas, ya que esto podría considerarse dentro de las expectativas razonables del interesado. Pero se debería exigir un consentimiento separado y adicional para permitir el envío de datos personales a terceros. La necesidad de más precisión en la obtención del consentimiento debe ser evaluada en cada caso concreto, según la(s) finalidad (es) o los destinatarios de los datos.

Hay que recordar que el tratamiento puede tener fundamentos jurídicos diferentes: algunos datos podrían tratarse por ser necesarios en el marco de un contrato con el interesado, para cumplir con los productos y gestionar el servicio, y podría requerirse un consentimiento específico para tratar datos más allá de lo necesario para ejecutar el contrato, como por ejemplo para evaluar la capacidad de pago (calificación crediticia) del interesado.

El Grupo de trabajo ha aclarado este aspecto del consentimiento en el documento WP131 sobre los historiales médicos electrónicos: el consentimiento «específico» debe referirse a una situación bien definida y concreta en que esté previsto el tratamiento de datos médicos. Por tanto, el «acuerdo genérico» del interesado, por ejemplo para la recogida de sus datos médicos para un historial médico electrónico y cualquier transferencia futura de estos datos médicos a los profesionales de la salud que intervengan en el tratamiento, no se considerará consentimiento en el sentido del artículo 2, letra h), de la Directiva.

El mismo razonamiento se hace en el dictamen WP115 sobre el uso de datos de localización con vistas a prestar servicios con valor añadido: «Esta definición descarta explícitamente que se otorgue el consentimiento como parte de la aceptación de las condiciones generales para el servicio de comunicaciones electrónicas ofrecido. ... « ... dependiendo del tipo de servicio ofrecido, el consentimiento puede referirse a una operación específica o puede constituir un acuerdo para poder ser localizado de forma permanente.»

En la decisión judicial anteriormente mencionada en el capítulo II sobre la «función del consentimiento», aunque el término «específico» no se utilice explícitamente, la explicación también insiste en la necesidad de consentimiento específico al declarar que «no basta con que el contrato de trabajo del interesado se refiera a un convenio colectivo que permita tal superación».

Ejemplo: redes sociales
El acceso a los servicios de redes sociales suele estar sujeto a la autorización de diferentes tipos de tratamiento de datos personales.

Al usuario se le puede pedir su consentimiento para recibir publicidad comportamental para inscribirse en un servicio de red social, sin más especificaciones ni opciones alternativas. Considerando la importancia que han adquirido algunas redes sociales, ciertas categorías de usuarios (como los adolescentes) aceptarán la recepción de publicidad comportamental para evitar el riesgo de ser parcialmente excluidos de las interacciones sociales. El usuario debería estar en condiciones de dar su consentimiento libre y específico para recibir la publicidad comportamental, independientemente de su acceso al servicio de la red social. Para ofrecer al usuario esta posibilidad podría utilizarse una ventana desplegable.

El servicio de red social ofrece la posibilidad de utilizar aplicaciones externas.« En la práctica, es frecuente que al usuario se le impida utilizar una aplicación si no da su consentimiento para la transmisión de sus datos al promotor de la aplicación para diversos motivos, incluida la publicidad comportamental y la reventa a terceros.
Dado que la aplicación puede funcionar sin necesidad de transmitir ningún dato al promotor de la aplicación, el Grupo de Trabajo propugna un mayor grado de precisión al obtener el consentimiento del usuario, es decir, un consentimiento del usuario diferenciado para la transmisión de sus datos al promotor para los diferentes fines. Podrían utilizarse diferentes mecanismos, como las ventanas desplegables, para que el usuario tuviera la posibilidad de seleccionar el uso de sus datos para el que da su consentimiento (transmisión al promotor, servicios de valor añadido; publicidad comportamental; transmisión a terceros; etc.).

El carácter específico del consentimiento también significa que si los fines para los que los datos son tratados por el responsable cambian en algún momento, el usuario deberá ser informado y estar en condiciones de dar su consentimiento para el nuevo tratamiento de datos. La información que se facilite deberá mencionar las consecuencias del rechazo de los cambios propuestos.

« [manifestación de voluntad] … informada ...» .

El último elemento de la definición de consentimiento - pero no el último requisito, como veremos a continuación - es la manifestación de una voluntad «informada».

Los artículos 10 y 11 de la Directiva establecen la obligación de proporcionar información a los interesados. La obligación de informar es, por lo tanto, diferente del consentimiento, aunque en muchos casos está obviamente vinculada a éste. Mientras que el consentimiento no siempre sigue al suministro de información (podría utilizarse otro fundamento jurídico del artículo 7), la información siempre es necesaria antes del consentimiento.

Esto significa en la práctica que «El consentimiento debe ser con conocimiento de causa: un consentimiento «informado» por parte del interesado supone un consentimiento basado en la apreciación y comprensión de los hechos y consecuencias de una acción. El individuo afectado debe contar con información exacta y completa, dada de forma clara y comprensible, sobre todas las cuestiones pertinentes, en especial las especificadas en los artículos 10 y 11 de la Directiva, tal como la naturaleza de los datos tratados, los fines del tratamiento de que van a ser objeto los datos, los destinatarios de los mismos y los derechos del interesado. Esto incluye también el conocimiento de las consecuencias de no consentir el tratamiento de los datos en cuestión»[23].

En muchos casos, el consentimiento se obtendrá en el momento de recogida de los datos personales, cuando el tratamiento comienza. Si es así, la información que debe facilitarse coincide con la enumerada en el artículo 10 de la Directiva. Ahora bien, el consentimiento puede también ser solicitado en la «fase posterior», cuando cambia la finalidad del tratamiento. En este caso, la información que debe facilitarse tendrá que centrarse en las necesidades del contexto específico en relación con la finalidad.

El consentimiento como manifestación de voluntad informada es especialmente importante en el contexto de las transmisiones de datos personales a terceros países: «exige que el interesado (esté) informado adecuadamente del riesgo particular de que sus datos se transfieran un país que carece de la protección adecuada»[24].

Para garantizar una información adecuada se requieren dos tipos de requisitos:

- Calidad de la información - la manera en que se presenta la información (texto claro, sin jerga, comprensible, visible) es esencial para determinar si el consentimiento es manifestación de voluntad «informada». La forma en que se suministra esta información depende del contexto: el usuario medio/habitual debe ser capaz de entenderla.

- Accesibilidad y visibilidad de la información – La información debe comunicarse directamente a las personas. No basta con que la información esté «disponible» en algún lugar. El Tribunal de Justicia ha insistido en este punto en su sentencia de 2004[25], en relación con un contrato laboral que incluía condiciones no redactadas en el contrato pero mencionadas en él. La información debe ser claramente visible (tipo y tamaño de los caracteres), destacada y completa. Las ventanas de diálogo pueden utilizarse para dar información específica en el momento en que se solicita el consentimiento. Tal como se ha mencionado anteriormente en relación con el «consentimiento específico», las herramientas de información en línea son especialmente útiles en los servicios de redes sociales para aportar la suficiente precisión y claridad a la configuración de la intimidad. Los avisos breves también puede ser un instrumento útil en este contexto, ya que contribuyen a dar la información correcta de manera fácilmente accesible.

A medida que pasa el tiempo pueden surgir dudas sobre la validez de un consentimiento que se basó en su origen en información válida y suficiente. La gente suele cambiar de opinión por motivos muy variados, porque la elección inicial se tomó a la ligera o debido a un cambio de circunstancias como que un niño alcance la madurez[26]. Por este motivo, y en aras de la buena práctica, los responsables del tratamiento deben procurar examinar, después de un cierto tiempo, las decisiones individuales, por ejemplo,

---

[23] WP131 - Documento de trabajo sobre el tratamiento de datos personales relativos a la salud en los historiales médicos electrónicos.

[24] WP12 - Documento de trabajo «Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE». Véase también WP114 - Documento de trabajo del Grupo del Artículo 29 sobre una interpretación común del artículo 26, apartado 1, de la Directiva 95/46/CE de 24 de octubre de 1995.

[25] Véase la nota a pie de página 12 (capítulo II.2)

[26] Documento de trabajo 1/2008, sobre la protección de los datos personales de los niños, WP 147, 18 de febrero de 2008.

informando a las personas de su opción actual y ofreciéndoles la posibilidad de confirmarla o de retirarse[27]. El período pertinente dependería obviamente del contexto y las circunstancias del caso.

Ejemplo: mapa de la delincuencia
Algunas fuerzas policiales están considerando la publicación de mapas o datos que muestren los lugares donde se han cometido determinados tipos de delitos. Generalmente, este proceso se basa en garantías de que no se publicarán datos personales de las víctimas de delitos, dado que la delincuencia sólo está vinculada a zonas geográficas relativamente extensas. Sin embargo, algunas fuerzas policiales quieren detectar los delitos con más precisión, cuando la víctima del delito da su consentimiento. En tal caso es posible relacionar de manera más precisa al interesado con el lugar de comisión del delito. Sin embargo, a la víctima no se le dice explícitamente que se publicará información identificable sobre ella de forma abierta en Internet ni la manera en que esta información puede utilizarse. Por lo tanto, el consentimiento no es válido en este caso, ya que las víctimas probablemente no entenderán plenamente el alcance de la información que se está publicando sobre ellas.

Cuanto más complejo sea el tratamiento de datos, más se podrá esperar del responsable de su tratamiento. Cuanto más difícil resulte para un ciudadano medio supervisar y comprender todos los elementos del tratamiento de datos, mayor debería ser el esfuerzo del responsable para demostrar que el consentimiento obtenido se basó en información específica y comprensible.

El consentimiento, tal como se define en el artículo 2, letra h), debe leerse junto con los otros requisitos mencionados posteriormente en el texto de la Directiva. El artículo 7 añade las palabras «de forma inequívoca» a los elementos de la definición, y el artículo 8 añade la palabra «explícito» cuando el tratamiento se refiere a categorías específicas de datos.

III.A.2. Artículo 7, letra a)

De conformidad con el artículo 7, letra a), de la Directiva, el consentimiento como manifestación de voluntad inequívoca del interesado constituye la base jurídica del tratamiento de datos personales. Así, para ser válido, además de los criterios establecidos en el artículo 2, letra h), el consentimiento también debe ser inequívoco.

Para que el consentimiento se otorgue de forma inequívoca, el procedimiento de su obtención y otorgamiento no tiene que dejar *ninguna duda* sobre la intención del interesado al dar su consentimiento. En otras palabras, la manifestación mediante la cual el interesado consiente no debe dejar lugar a ningún equívoco sobre su intención. Si existe una duda razonable sobre la intención de la persona se producirá una situación equívoca.

[27] El Grupo del Artículo 29 hace una recomendación similar en el artículo 29 del Dictamen 171 sobre la publicidad comportamental en línea, adoptado el 22.6.2010.

Como se describe a continuación, este requisito obliga a los responsables del tratamiento a crear procedimientos rigurosos para que las personas den su consentimiento; se trata de, o bien buscar un claro consentimiento expreso o bien basarse en determinados tipos de procedimientos para que las personas manifiesten un claro consentimiento deducible. El responsable del tratamiento debe además asegurarse suficientemente de que la persona que da su consentimiento es efectivamente el interesado. Esto tiene especial importancia cuando el consentimiento se autoriza por teléfono o en línea.

La prueba del consentimiento plantea una cuestión relacionada con lo anterior. Los responsables del tratamiento que se basen en el consentimiento pueden desear o necesitar demostrar que el consentimiento se ha obtenido, por ejemplo, en el contexto de un litigio con el interesado. Efectivamente, en algunos casos se les podrá pedir que aporten estas pruebas en el marco de medidas ejecutivas. Como consecuencia de ello y como cuestión de buena práctica los responsables del tratamiento deben crear y conservar pruebas de que el consentimiento fue efectivamente dado, lo que significa que el consentimiento debería ser demostrable.

A continuación se analizan los siguientes métodos para dar el consentimiento y determinar si generan un consentimiento inequívoco.

Las manifestaciones expresas del consentimiento tales como un acuerdo firmado o manifestaciones escritas de la voluntad de llegar a un acuerdo son procedimientos o mecanismos adecuados para generar un consentimiento inequívoco. En principio, también proporcionan pruebas al responsable del tratamiento de que se ha obtenido el consentimiento.

Ejemplo: consentimiento para recibir información de promoción por correo postal

Un hotel pide a los particulares que indiquen su dirección postal en un formulario de papel si desean recibir información de promoción por correo postal. Si la persona, después de facilitar la información postal, firma el formulario para indicar su acuerdo, estará dando su consentimiento inequívoco. En este caso, el consentimiento será expreso y por escrito. Este procedimiento proporciona al responsable del tratamiento la prueba de haber obtenido el consentimiento de todos los clientes si conserva todos los formularios firmados.

Sin embargo, no todas las formas de acuerdo que pueden parecer explícitas generarán consentimiento. Esta cuestión fue examinada en el asunto reciente del TJCE (Volker und Markus schecke contra Land de Hesse), que se refiere a la publicación de los nombres de los beneficiarios de distintos fondos[28] de la UE y de las cantidades recibidas por cada beneficiario. El Abogado General examinó si las condiciones para el consentimiento inequívoco se cumplían en un caso en que las personas habían firmado una declaración que decía: «Me consta que, conforme al artículo 44 bis del Reglamento (CE) nº 1290/2005, es obligatorio publicar los datos de los beneficiarios del FEAGA y del Feader y los importes recibidos por cada beneficiario.» El Abogado General concluía: «El reconocimiento de haber sido informado de que se va a producir alguna clase de publicación no es lo mismo que dar un consentimiento "inequívoco" a una clase específica de publicación detallada. Y tampoco puede describirse como una

[28] Fondo Europeo Agrícola de Garantía (FEAGA) y Fondo Europeo Agrícola de Desarrollo Rural (FEADER).

«manifestación libre y específica» de la voluntad del interesado de conformidad con la definición del consentimiento del interesado que recoge el artículo 2, letra h).» Concluyó, por lo tanto, que los solicitantes no había dado su consentimiento al tratamiento (es decir, la publicación) de sus datos personales en el sentido del artículo 7, letra a), de la Directiva 95/46/CE[29].

El consentimiento explícito también puede darse en el entorno de los servicios en línea. Al igual que en el entorno fuera de línea, existen medios muy idóneos para dar el consentimiento explícito, como ilustra el siguiente ejemplo.

Ejemplo: consentimiento en línea para adherirse a un programa de fidelidad
El sitio *web* de un hotel incluye un formulario de reserva que permite a los clientes reservar habitaciones por adelantado por vía electrónica. El formulario en línea en el que los clientes introducen las fechas de reserva y los datos de pago también incluye una casilla visible que deben marcar los clientes que desean que sus datos se utilicen para inscribirse en un programa de fidelidad. Marcar la casilla tras haber recibido la información pertinente constituye un consentimiento explícito e inequívoco, ya que la acción de marcar la casilla es suficientemente clara para no dejar lugar a dudas sobre el deseo de la persona de adherirse al programa de fidelidad.

El consentimiento expreso también puede darse verbalmente, mediante declaraciones destinadas a expresar acuerdo. El consentimiento verbal explícito se concedería en la situación siguiente.

Ejemplo: consentimiento verbal para recibir información sobre promociones
En el momento de pagar en la recepción del hotel, el empleado pregunta a los clientes si desean dejar su dirección para que el hotel les comunique las promociones. Las personas que respondan facilitando su dirección postal, después de haber oído al empleado y disponer de la información pertinente, estarían dando su consentimiento explícito. La acción de comunicar la dirección puede constituir una manifestación inequívoca de la voluntad individual. No obstante, el responsable del tratamiento de datos puede optar por aplicar mecanismos que demuestren de forma más fiable que se ha dado el consentimiento.

En algunas circunstancias, el consentimiento inequívoco puede deducirse de determinadas acciones, en particular cuando las acciones conducen a la conclusión inequívoca de que ha habido consentimiento. Sin embargo, esto depende de que se haya suministrado información pertinente sobre el tratamiento que permita a la persona tomar una decisión (persona responsable del tratamiento, finalidades del tratamiento, etc.).

[29] Conclusiones del Abogado General Sharpston publicadas el 17 de junio de 2010, Volker und Markus S GbR, en los asuntos acumulados C-92/09 y C-93/09. Hay que señalar que el TJUE, en su sentencia de 9 de noviembre de 2010 declaró que el tratamiento de los datos no se basaba en el consentimiento: «63. La normativa de la Unión controvertida, que se limita a disponer que se informará previamente a los beneficiarios de las ayudas de que sus datos serán publicados, no pretende, pues, basar el tratamiento de los datos personales regulado por ella en el consentimiento de los beneficiarios afectados.»

.

Ejemplo: consentimiento para ser fotografiado
Al realizar la inscripción en la recepción del hotel, el empleado informa a los clientes de que por la tarde tendrá lugar una sesión fotográfica en una de las cafeterías del hotel. Las imágenes que se seleccionen se utilizarán como material comercial, especialmente para los folletos del hotel en soporte papel. Si los huéspedes del hotel desean ser fotografiados, se les invita a la cafetería a la hora prevista. Se dispone de otra cafetería para aquellos que no deseen ser fotografiados.

Se considera que los huéspedes del hotel que han sido informados y deciden ir a la cafetería durante la sesión fotográfica dan su consentimiento para ser fotografiados. Su consentimiento se deduce de la acción de acudir a la cafetería cuando tiene lugar la sesión fotográfica a la hora prevista. Acudir a la cafetería constituye una manifestación de voluntad de la persona que, en principio, puede considerarse inequívoca, pues no cabe duda de que acude a la cafetería para ser fotografiada. Sin embargo, el hotel podría considerar prudente disponer de pruebas escritas del consentimiento obtenido, en caso de que la validez del consentimiento se cuestione en un futuro próximo.

Como ya se ha mencionado, los mismos requisitos, incluido el consentimiento inequívoco, se aplican tanto en línea como en contextos fuera de línea. Sin embargo, el Grupo de Trabajo considera que el riesgo de consentimiento equívoco es mayor en el entorno en línea, que requiere especial atención. El siguiente ejemplo ilustra un caso en que el consentimiento que se deduce de una acción concreta (participación en un juego en línea) no cumple los requisitos de validez del consentimiento.

Ejemplo: juego en línea
El proveedor de un juego en línea exige a los jugadores que faciliten su edad, nombre y dirección para participar en el juego (distribución de jugadores por edades y direcciones). El sitio *web* contiene un anuncio, accesible a través de un enlace (aunque el acceso al anuncio no es necesariamente para participar en el juego), que indica que al utilizar el sitio *web* (y, por tanto, al facilitar información) los jugadores consienten en que sus datos sean tratados para que el proveedor de juegos en línea y terceros les envíen información comercial.

El acceso y la participación en el juego no equivale a dar un consentimiento inequívoco para el ulterior tratamiento de la información personal con fines distintos de la participación en el juego. La participación en el juego no implica que la persona tiene la intención de dar su consentimiento para un tratamiento distinto al necesario para el juego. Este tipo de comportamiento no constituye una manifestación inequívoca del deseo de la persona de que sus datos se utilicen para fines comerciales.

Ejemplo: parámetros de privacidad por defecto
Los parámetros por defecto de una red social, a los que los usuarios no acceden necesariamente al utilizarla, permiten a la totalidad de la categoría «amigos de amigos» hacer que toda la información personal de cada usuario pueda ser vista por todos los «amigos de amigos». Los usuarios que no desean que su información sea vista por los «amigos de amigos» tienen que pulsar un botón. El responsable del tratamiento considera que si se abstienen de actuar o no pulsan el botón han consentido en que se puedan ver sus datos. Sin embargo, es muy cuestionable que *no* pulsar el botón signifique que por lo general las personas *consienten* en que su información pueda ser vista por todos los amigos de amigos. Debido a la incertidumbre en cuanto a si la inacción significa consentimiento, el hecho de no pulsar no puede considerarse consentimiento inequívoco.

Este ejemplo ilustra el caso de la persona que permanece pasiva (por ejemplo, inacción o «silencio»). El consentimiento inequívoco no encaja bien con los procedimientos para obtener el consentimiento a partir de la inacción o el silencio de las personas: el silencio o la inacción de una parte es intrínsecamente equívoco (la intención del interesado podría ser de asentimiento o simplemente no realizar la acción). El siguiente ejemplo ilustra lo anterior.

Es equívoca la situación en que se considera que las personas han dado su consentimiento si no han contestado a una carta cuando estaban informadas de que la falta de respuesta equivalía a consentir. En este tipo de situaciones, el comportamiento individual (o más bien, la falta de acción), plantea serias dudas sobre la voluntad de acuerdo de la persona. El hecho de que la persona no realice una acción positiva no permite concluir que ha dado su consentimiento. Por tanto, no cumple el requisito de consentimiento inequívoco. Además, como se ilustra a continuación, también será muy difícil para el responsable del tratamiento de datos aportar la prueba que demuestre que la persona ha consentido.

El Grupo de trabajo ha declarado la inadecuación del consentimiento basado en el silencio de la persona en el contexto del envío directo de publicidad por mensajes electrónicos. «El consentimiento implícito para recibir tales mensajes no es compatible con la definición de consentimiento establecida en la Directiva 95/46/CE ... De forma similar, las casillas preseleccionadas, p. ej. en sitios *web*, tampoco son compatibles con la definición de la Directiva»[30]. El siguiente ejemplo confirma esta opinión:

Ejemplo: invalidez del consentimiento para usos adicionales de datos de clientes
Una librería en línea envía mensajes electrónicos a sus clientes que participan en un programa de fidelidad informándoles de que sus datos serán transferidos a una empresa publicitaria que los utilizará para fines comerciales. Los usuarios tienen dos semanas para contestar al mensaje electrónico. Se les informa de que la falta de respuesta se considerará consentimiento de la transferencia. Este tipo de mecanismo, mediante el cual el consentimiento se deduce de la falta de reacción de las personas, no genera un consentimiento válido ni inequívoco. No es posible determinar sin lugar a dudas que las personas han consentido la transferencia por su falta de respuesta.

[30] Dictamen 5/2004 sobre comunicaciones no solicitadas con fines de venta directa con arreglo al artículo 13 de la Directiva 2002/58/CE, adoptada el 27 de febrero de 2004 (WP90).

Se deduce de lo anterior que, habida cuenta del carácter inequívoco que debe tener el consentimiento, se anima de hecho a los responsables del tratamiento a aplicar procedimientos y mecanismos que no dejen ninguna duda de que el consentimiento se ha dado, bien sobre la base de una acción expresa realizada por la persona, bien por deducirse claramente de una acción realizada por la persona.

Según lo anterior, los responsables del tratamiento, en aras de las buenas prácticas, deben considerar la posibilidad de adoptar medidas y procedimientos pertinentes para demostrar que se ha dado el consentimiento. Cuanto más complicados sean los entornos en los que actúan, más medidas serán necesarias para garantizar que el consentimiento puede demostrarse. Esta información debería ponerse a disposición de la autoridad de protección de datos, previa solicitud.

III.A.3. <u>Artículo 8, apartado 2, letra a)</u>

El artículo 8 de la Directiva prevé una protección especial para las «categorías especiales de datos» consideradas de naturaleza muy sensible. Se prohíbe el tratamiento de estos datos salvo en caso de que se aplique al menos una de las excepciones establecidas. El artículo 8, apartado 2, letra a), establece que la prohibición no se aplicará cuando el interesado haya dado su «consentimiento explícito» al tratamiento.

Jurídicamente, el término «consentimiento explícito» significa lo mismo que el consentimiento expreso. Abarca todas las situaciones en las que se propone a la persona que consienta o no un uso particular o la difusión de su información personal y la persona responde de forma activa a la pregunta, verbalmente o por escrito. Por lo general, el consentimiento explícito o expreso se da por escrito y se firma a mano. Por ejemplo, se da el consentimiento explícito cuando los interesados firman un formulario de consentimiento que especifica claramente los motivos por los que el responsable del tratamiento desea recopilar y seguir tratando datos personales.

Tradicionalmente, el consentimiento explícito ha sido escrito, en papel o en soporte electrónico, como ya se ha mencionado en el capítulo III.A.2, pero no tiene que ser necesariamente así, ya que también puede ser verbal. Así lo confirma el hecho de que el requisito del consentimiento escrito, que se propuso en el artículo 8, fuera suprimido en la última versión de la Directiva. Ahora bien, como se explica en el mismo capítulo, el consentimiento verbal puede ser difícil de demostrar, por lo que en la práctica se pide a los responsables que utilicen el consentimiento escrito a efectos probatorios.

El requisito del consentimiento explícito implica que, por lo general, el consentimiento que se infiere no cumple los requisitos del artículo 8, apartado 2. A este respecto, conviene recordar que el dictamen del Grupo del artículo 29 relativo a los historiales médicos electrónicos[31] afirma que «En contraste con lo previsto en el artículo 7 de la Directiva, el consentimiento en el caso de los datos personales sensibles y por tanto de un HME

[31] WP131 - Documento de trabajo sobre el tratamiento de datos personales relativos a la salud en los historiales médicos electrónicos (HME).

debe ser **explícito.** Las soluciones consistentes en entender que existe una autorización tácita si no se manifiesta explícitamente lo contrario, no cumplirán el requisito de ser «explícitas» … ».

Ejemplo: datos médicos para la investigación
El paciente al que la clínica informa de que su expediente médico será transferido a un investigador salvo objeción por su parte (a través del teléfono), no cumple el requisito del consentimiento explícito.

Como se ha indicado en el capítulo II.A.2, las personas pueden dar su consentimiento explícito verbalmente y por escrito mediante un acto afirmativo que exprese su deseo de aceptar un tipo de tratamiento de datos. En el entorno electrónico, el consentimiento explícito puede darse mediante firmas electrónicas o digitales. También puede darse pulsando botones según el contexto, enviando mensajes electrónicos de confirmación, pinchando en iconos, etc[32]. Los procedimientos que implican una acción afirmativa de la persona se confirman en el considerando 17 de la Directiva sobre privacidad, que establece: «El consentimiento podrá darse por cualquier medio apropiado que permita la manifestación libre, inequívoca y fundada de la voluntad del usuario, por ejemplo mediante la selección de una casilla de un sitio *web* en Internet».

Para ser válido, no es necesario que el consentimiento pueda registrarse. Ahora bien, al responsable del tratamiento le interesa conservar la prueba. Es obvio que los mecanismos específicos tienen una fuerza probatoria que puede variar y demostrar en mayor o menor medida el consentimiento. El consentimiento obtenido pulsando un botón basado en la identidad de una persona extraída de una dirección electrónica tendrá mucha menos fuerza probatoria que un proceso similar basado en mecanismos registrables del consentimiento[33]. La necesidad de disponer de pruebas sólidas dependerá también del tipo de datos recogidos y del propósito perseguido: la firma electrónica no se requerirá para dar el consentimiento para recibir ofertas comerciales, pero puede ser necesaria para consentir el tratamiento de determinados tipos de datos financieros en línea. El consentimiento explícito dado en el contexto en línea deberá ser registrable para poder acceder a él en ulteriores ocasiones[34].

A la vista de lo anterior, se considerará que los formularios de inscripción en línea que deben cumplimentar las personas con sus datos y su acuerdo para el tratamiento

[32] Esta interpretación concuerda con la normativa de la UE, especialmente en lo que respecta al comercio electrónico y al uso creciente de las firmas electrónicas, que ha exigido a los Estados miembros modificar sus normativas que regulan los requisitos formales de los documentos «escritos» o «manuscritos», a fin de admitir igualmente a sus interlocutores electrónicos, siempre que se cumplan determinadas condiciones.

[33] A este respecto, véase por ejemplo las Leyes griega y alemana sobre los requisitos del consentimiento por medios electrónicos, que requieren que el consentimiento se registre en condiciones de seguridad, y prevén la posibilidad de acceso del usuario o abonado en cualquier momento y de revocación en cualquier momento [artículo 5, apartado 3, de la Ley griega 3471/2006 sobre la protección de datos personales en el sector de las comunicaciones electrónicas; el artículo 13, apartado 2, de la Ley alemana de teleservicios, el artículo 94 de la Ley alemana de telecomunicaciones y el artículo 28, apartado 3, letra a), de la Ley federal alemana de protección de datos].

[34] No entra en el ámbito del presente Dictamen analizar las condiciones técnicas que deben cumplir los documentos electrónicos y las firmas electrónicas para que pueda otorgárseles el mismo valor probatorio que los equivalentes escritos a mano. Este asunto va más allá de la normativa de protección de datos y ha sido regulado en el ámbito de la UE.

cumplen el requisito de consentimiento explícito, siempre que reúnan también todos los demás requisitos. Por ejemplo, para abrir un expediente médico personalizado en línea, los pacientes pueden dar su consentimiento facilitando sus datos de contacto y señalando una casilla específica para manifestar su acuerdo. La utilización de métodos de autenticación más rigurosos – como las firmas digitales - producirá resultados parecidos que tendrán mayor fuerza probatoria[35].

En algunos casos, los Estados miembros pueden decidir legitimar una determinada operación de tratamiento sobre la base del consentimiento y especificar el tipo de consentimiento. Por ejemplo, para solicitar una tarjeta sanitaria que permita acceder al historial médico, los Estados miembros pueden decidir que las personas que se registren en línea utilicen una firma digital particular. Esta opción garantizará la rapidez del consentimiento. Asimismo, el responsable del tratamiento estará en condiciones de comprobar el consentimiento de la persona.

III.A.4. <u>Artículo 26, apartado 1</u>

El artículo 26, apartado 1, letra a), establece que el consentimiento inequívoco del interesado es una excepción a la prohibición de transferir datos a terceros países que no ofrezcan garantías. La reflexión anterior sobre el artículo 7, letra a), se aplica también aquí. Es decir, además de los requisitos de validez del consentimiento del antiguo artículo 2, letra g), el consentimiento debe ser inequívoco.

El Grupo del artículo 29 ha realizado un gran esfuerzo para impartir directrices sobre la aplicación de los artículos 25 y 26 de la Directiva, incluida la excepción del consentimiento. En este contexto, conviene recordar lo que dice el documento WP12[36] del Grupo de trabajo en relación con el significado del consentimiento inequívoco:
«Puesto que el consentimiento debe ser inequívoco, cualquier duda sobre su obtención anularía la aplicabilidad de la excepción. Esto podría significar que en muchas situaciones en que el consentimiento se da por sobreentendido (por ejemplo, porque la persona ha sido informada de una transferencia y no se ha opuesto), la excepción no resultaría aplicable».

A la luz de lo anterior, será más probable obtener el consentimiento inequívoco cuando las personas realicen acciones afirmativas para mostrar su acuerdo con la transferencia, como por ejemplo firmar un formulario de consentimiento o realizar otras acciones que no dejen lugar a dudas sobre el consentimiento otorgado.

En el documento WP 114[37], el Grupo de trabajo se refiere al uso del consentimiento para las transferencias de datos en los siguientes términos: «es improbable que el consentimiento ofrezca un marco adecuado a largo plazo para los responsables del tratamiento en casos de transferencias repetidas o incluso estructurales para el

35 Esto es así porque a determinados tipos de firmas digitales (firmas electrónicas avanzadas que se basan en un certificado cualificado y se crean mediante un dispositivo de creación de firma segura) se les supone el mismo valor jurídico que a las firmas escritas.

36 WP12 – Documento de trabajo sobre transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva de la UE sobre protección de datos, adoptada el 24 de julio de 1998.

37 Documento de trabajo relativo a una interpretación común del artículo 26, apartado 1, de la Directiva 95/46/CE, de 24 de octubre de 1995, adoptado el 25.11.2005.

tratamiento de que se trate. De hecho, especialmente si la transferencia es parte intrínseca del tratamiento principal (por ejemplo, centralización de una base de datos de recursos humanos a escala mundial, que, para ser operativa, ha de ser alimentada mediante transferencias de datos de forma permanente y sistemática), cabe la posibilidad de que los responsables del tratamiento se encuentren en situaciones insolubles, si sólo uno de los interesados decidiese con posterioridad retirar su consentimiento. En rigor, ya no podrían ser transferidos los datos relativos a una persona que haya retirado su consentimiento; de no ser así, la transferencia seguiría basándose parcialmente en el consentimiento del interesado, si bien habría que encontrar una solución alternativa (un contrato, normas corporativas vinculantes, etc.) para los datos relativos a interesados que hayan retirado su consentimiento. Por consiguiente, es posible que basarse en el consentimiento constituya una «falsa buena solución», simple a primera vista pero compleja y engorrosa en realidad.»

III.A.4. El consentimiento de las personas sin capacidad jurídica

La Directiva 95/46/CE no establece ninguna disposición particular sobre la obtención del consentimiento de las personas que no tienen capacidad jurídica, incluidos los niños. Es importante tener en cuenta esta realidad a la hora de modificar la Directiva sobre protección de datos. Además de las cuestiones anteriormente mencionadas, el consentimiento de estas personas plantea sus propios problemas específicos.

En cuanto a los niños, las condiciones de validez de su consentimiento difieren de un Estado miembro a otro. El Grupo de trabajo del artículo 29 ha reflexionado en varias ocasiones sobre el consentimiento de los niños y ha examinado las prácticas nacionales[38].

Los estudios muestran que los requisitos jurídicos para obtener el consentimiento de los niños pueden consistir en obtener el consentimiento del menor y su representante o únicamente el consentimiento del menor que ya ha adquirido madurez. Las edades exigidas para aplicar las diversas normas también varían. No existe ningún procedimiento armonizado para comprobar la edad del niño.

La ausencia de normas generales conduce a un enfoque fragmentario que no reconoce la necesidad de protección específica de los niños en circunstancias específicas, habida cuenta de su vulnerabilidad, y genera inseguridad jurídica, especialmente en cuanto a la forma de obtener el consentimiento del niño.

El Grupo de trabajo considera que la falta de armonización afecta a la seguridad jurídica. La armonización de las condiciones exigidas a las personas sin capacidad jurídica para ejercer sus derechos en el ámbito de la UE, especialmente en lo que respecta al límite de edad, aportaría ciertamente garantías adicionales. No obstante, el Grupo de trabajo es consciente de que el asunto va más allá del ámbito de la protección de datos, ya que se trata, en general, de cuestiones de Derecho civil. El Grupo desea llamar la atención de la Comisión sobre los retos que se plantean al respecto.

[38] WP147 – Documento de trabajo 1/2008 sobre la protección de los datos personales de los niños (Directrices generales y especial referencia a las escuelas); WP160 – Dictamen 2/2009 sobre la protección de los datos personales de los niños (Directrices generales y especial referencia a las escuelas).

Además, el Grupo del artículo 29 considera que los intereses de los niños y otras personas sin capacidad jurídica plena podrían protegerse mejor si la Directiva recogiera disposiciones adicionales relativas específicamente a la recopilación y el tratamiento posterior de sus datos. Dichas disposiciones podrían prever las circunstancias en que se requiere el consentimiento del representante, conjuntamente con o en lugar del consentimiento de la persona sin capacidad, así como las circunstancias en las que no se debería utilizar el consentimiento para legitimar el tratamiento de datos personales. Asimismo, deberían establecer el requisito de aplicación de mecanismos electrónicos de comprobación de la edad. Existen diferentes mecanismos y límites. Por ejemplo, la comprobación de la edad, más que estar sujeta a una única norma, podría basarse en una escala móvil en virtud de la cual el mecanismo a utilizar dependería de circunstancias como el tipo de tratamiento (finalidades), el nivel de riesgos, el tipo de datos recopilados, los usos de los datos (si está prevista su difusión), etc.

III.B. Directiva 2002/58/CE

La Directiva sobre privacidad (Directiva 2002/58/CE)[39] recientemente modificada constituye una *lex specialis* respecto de la Directiva 95/46/CE en la medida en que contiene un régimen de sector específico de la privacidad y las comunicaciones electrónicas. La mayoría de sus disposiciones se aplica únicamente a los proveedores de servicios de comunicaciones electrónicas disponibles al público (por ejemplo, proveedores de telefonía, servicios de Internet, etc.).

Algunas disposiciones de la Directiva sobre privacidad se basan en el consentimiento como fundamento jurídico del tratamiento de datos por parte de los servicios de comunicaciones electrónicas disponibles al público[40]. Así ocurre, por ejemplo, con el uso de los datos de tráfico o de localización.

El Grupo de trabajo del artículo 29 considera útil comentar algunos aspectos del uso del consentimiento en la Directiva sobre privacidad que le parecen especialmente interesantes. A tal fin, trataremos las cinco cuestiones siguientes:

a) la relación entre la definición y el significado general del consentimiento en la Directiva 95/46/CE y la Directiva sobre privacidad. El análisis se basa en el artículo 2, apartado 2, letra f), de la Directiva sobre privacidad.

b) La necesidad o no de obtener el consentimiento de una o ambas partes de la comunicación en caso de que se pretenda suspender la confidencialidad de las comunicaciones (por ejemplo, para seguir o interceptar una comunicación telefónica). Esto se regula en el artículo 6, apartado 3, y artículo 5, apartado 1.

---

[39] Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009 , por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) n o 2006/2004 sobre la cooperación en materia de protección de los consumidores, De 18.12.2009.

[40] Datos de tráfico son los datos tratados con el fin de realizar una comunicación en una red de comunicaciones electrónicas o la facturación de esta comunicación, incluidos los datos relativos a la transferencia, la duración o la fecha y hora de la comunicación.

c) La cuestión de los plazos para la obtención del consentimiento. Esta cuestión se aborda en diversas disposiciones de la Directiva sobre privacidad, incluidos su artículo 5, apartado 3) y artículos 6 y 13.

d) El ámbito de aplicación del derecho de oposición y su distinción respecto del consentimiento. Esta distinción puede analizarse en el marco del artículo 13 de la Directiva sobre privacidad.

d) La posibilidad de retirar el consentimiento tal como está previsto explícitamente en el artículo 6, apartado 3 y el artículo 9, apartados 3 y 4, de la Directiva sobre privacidad.

III.B.1. Artículo 2, letra f) - Consentimiento y relación con la Directiva 95/46/CE

«consentimiento de un usuario o abonado».

El artículo 2 de la Directiva sobre privacidad establece expresamente que las definiciones de la Directiva 95/46/CE se aplicarán en lo que respecta a la Directiva 2002/58/CE. Con arreglo al artículo 2, letra f), se entiende por « «consentimiento» de un usuario o abonado: el consentimiento del interesado, con arreglo a la definición de la Directiva 95/46/CE.»

Esto significa que cuando se requiera el consentimiento en virtud de la Directiva sobre privacidad, los criterios para determinar si el consentimiento es válido son los mismos que establece la Directiva 95/46/CE, a saber, la definición recogida en el artículo 2, letra g), y la especificidad incluida en el artículo 7, letra a). La idea de que el consentimiento en la Directiva sobre privacidad debe entenderse con referencia al artículo 2, letra g), y al artículo 7, letra a), conjuntamente, se confirma en el considerando 17[41].

III.B.2. Artículo 5, apartado 1. Necesidad o no del consentimiento de una o ambas partes

«… consentimiento de los usuarios interesados …»

El artículo 5, apartado 1, de la Directiva sobre privacidad protege la confidencialidad de las comunicaciones por medio de la prohibición de cualquier tipo de intervención o vigilancia de las comunicaciones sin el consentimiento de todos los usuarios interesados.

En este caso, el artículo 5, apartado 1), requiere el consentimiento de «los usuarios interesados», es decir, de las dos partes de la comunicación. El consentimiento de una parte no es suficiente.

[41] Dispone lo siguiente: «A efectos de la presente Directiva, el consentimiento … debe tener el mismo significado que el consentimiento de la persona afectada por los datos tal como se define y se especifica en la Directiva 95/46/CE.»

En el marco de la elaboración de su Dictamen 2/2006[42], el Grupo del Artículo 29 indagó sobre varios servicios que realizan el cribado del contenido del correo electrónico y, en algunos casos, el seguimiento de la apertura de mensajes. El Grupo manifestó su preocupación por el hecho de que en dichos servicios una de las partes de la comunicación no está informada. Para cumplir el artículo 5, apartado 1, es necesario que estos servicios cuenten con el consentimiento de ambas partes de la comunicación.

III.B.3 Artículo 6, apartado 3, artículos 9, 13 y 5, apartado 3, – plazos para requerir el consentimiento

"... « ... que se facilite … información clara y completa,...»

Diversas disposiciones de la Directiva sobre privacidad contienen implícita o explícitamente la exigencia de que el consentimiento debe darse antes del tratamiento. Esto concuerda con la Directiva 95/46/CE.

El artículo 6, apartado 3, de la Directiva sobre privacidad incluye una referencia explícita al consentimiento previo del abonado o del usuario interesado, y establece la obligación de suministrar información y obtener el consentimiento previo antes de efectuar el tratamiento de datos de tráfico para los fines de los servicios de comunicaciones electrónicos o los servicios de valor añadido. Para determinados tipos de servicios, se puede obtener el consentimiento de los abonados en el momento de suscribir el servicio. En otros casos, puede ser factible obtenerlo directamente del usuario. El artículo 9 adopta un enfoque similar del tratamiento de datos de localización distintos de datos de tráfico. El proveedor de servicios debe informar a los usuarios o abonados - «antes de obtener el consentimiento» - del tipo de datos de localización distintos de los datos de tráfico, que «serán» tratados. El artículo 13 establece el requisito de obtener el consentimiento previo de los abonados para la utilización de sistemas de llamada automática sin intervención humana, fax o correo electrónico con fines de venta directa.

El artículo 5, apartado 3, contiene una disposición específica sobre el almacenamiento de información o la obtención de acceso a la información almacenada en el equipo terminal de un usuario, con el fin particular de realizar el seguimiento de las actividades en línea del usuario. El artículo 5, apartado 3, no emplea la palabra «previamente», aunque ésta se deduce lógica y claramente del texto de la disposición.

Es de sentido común que el consentimiento ha de obtenerse «previamente» al inicio del tratamiento de datos. De otra forma, el tratamiento que se realizara durante el tiempo comprendido entre el momento en que comienza el tratamiento y el momento en que se obtiene el consentimiento sería ilegal por falta de base jurídica. Además, en tales casos, si la persona decidiera no dar su consentimiento, todo el tratamiento de datos ya realizado sería ilegal por esta razón.

Se deduce de lo anterior que, siempre que se requiera, el consentimiento deberá ser anterior al comienzo del tratamiento de datos. La posibilidad de iniciar el tratamiento sin haber obtenido antes el consentimiento sólo es legal cuando la Directiva de

42 Dictamen 2/2006 sobre en respeto de la privacidad en relación con la prestación de servicios de cribado de correo electrónico, adoptado el 21.2.2006 (WP118).

protección de datos o la Directiva sobre privacidad, en lugar de exigir el consentimiento, prevé un fundamento alternativo y se refiere al derecho de oposición o a la negativa al tratamiento. Estos mecanismos se distinguen claramente del consentimiento. En estos casos, el tratamiento ya podría haber empezado y la persona tiene derecho a oponerse o a rechazarlo.

Un ejemplo de esto se encuentra en el artículo 5, apartado 3, de la antigua Directiva sobre privacidad, que establecía (el subrayado es nuestro): «que únicamente se permita el uso de las redes de comunicaciones electrónicas con fines de almacenamiento de información o de obtención de acceso a la información almacenada en el equipo terminal de un abonado o usuario a condición de que se facilite a dicho abonado o usuario información clara y completa, en particular sobre los fines del tratamiento de los datos, con arreglo a lo dispuesto en la Directiva 95/46/CE y de que el responsable del tratamiento de los datos <u>le ofrezca el derecho de negarse a dicho tratamiento</u>.» Esto debe compararse con la nueva redacción del artículo 5, apartado 3, de la Directiva sobre privacidad, modificada por la Directiva 2009/136/CE[43], que establece que « (…) únicamente se permita el almacenamiento de información, o la obtención de acceso a la información ya almacenada, en el equipo terminal de un abonado o usuario, a condición de que dicho abonado o usuario haya dado su consentimiento (…)». Las consecuencias de esta nueva redacción del artículo 5, apartado 3, las ha explicado el Grupo del Artículo 29 en su Dictamen 2/2010 sobre publicidad comportamental en línea[44]. La diferencia entre negativa y consentimiento se desarrolla en el próximo capítulo.

En muchos casos, la Directiva sobre privacidad o la Directiva sobre protección de datos prevé la posibilidad de negarse al tratamiento de datos de carácter personal debido a que la base jurídica del tratamiento inicial reside en fundamentos jurídicos *distintos* del consentimiento, como puede ser la existencia de un contrato. Además, esto se ilustra en la siguiente sección, que analiza el artículo 13 de la Directiva sobre privacidad.

III.B.4. <u>Artículo 13, apartados 2 y 3 – el derecho de oposición y su diferencia respecto del consentimiento</u>

« … que se ofrezca con absoluta claridad a los clientes, … y de manera sencilla, la posibilidad de oponerse …»

El artículo 13 de la Directiva sobre privacidad prevé utilizar el consentimiento para el envío de comunicaciones electrónicas con fines de venta legal. Para hacerlo, se basa en un principio estándar y una disposición específica.

[43] Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009 , por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) n o 2006/2004 sobre la cooperación en materia de protección de los consumidores. Texto pertinente a los fines del EEE, DO L 337 de 18.12.2009, p. 1100 – 0036.

[44] Dictamen de 22 de junio de 2010, WP 171: La cuestión de si el consentimiento puede expresarse mediante « el uso de los parámetros adecuados del navegador o de otra aplicación» [considerando 66 de la Directiva 2009/136/CE] se trata expresamente en el punto 4.1.1 del documento WP 171.

Para el uso de llamadores automáticos, faxes y mensajes electrónicos, exige el consentimiento del interesado.

Si el destinatario de la comunicación comercial es un cliente y la comunicación pretende promocionar los propios productos o servicios del proveedor u otros similares, no se exige el consentimiento sino ofrecer a las personas «la oportunidad de oponerse», con arreglo al antiguo artículo 13, apartado 2. El considerando 41 explica el razonamiento que lleva al legislador a no exigir en este caso el consentimiento: «En el contexto de una relación preexistente con el cliente, es razonable admitir el uso de las señas electrónicas del cliente con objeto de ofrecer productos o servicios similares». Así, en principio, la relación contractual entre la persona y el proveedor de servicios es el fundamento jurídico que permite el primer contacto por correo electrónico. Pero las personas deberían tener la posibilidad de oponerse a contactos posteriores. Como ha indicado el Grupo de trabajo: «Debe seguir ofreciéndose al cliente esta posibilidad cada vez que reciba un mensaje ulterior de venta directa, sin cargo alguno salvo los posibles costes de transmisión de esta negativa»[45].

Hay que distinguir entre la necesidad del consentimiento y el derecho a oponerse. Como se ha explicado anteriormente en el capítulo III.A.2, el consentimiento basado en la inacción de la persona, por ejemplo a través de casillas preseleccionadas, no cumple los requisitos de validez del consentimiento previstos en la Directiva 95/46/CE. La misma conclusión se aplica a los parámetros de navegador que aceptan por defecto que se seleccione al usuario (mediante el uso de *cookies*). Esto ha quedado claro en la nueva redacción del artículo 5, apartado 3, a la que nos hemos referido anteriormente en el capítulo III.B.3. En estos dos ejemplos no se cumplen los requisitos exigidos para una manifestación de voluntad inequívoca. Es fundamental que el interesado tenga la oportunidad de adoptar una decisión y manifestarla, por ejemplo seleccionado él mismo la casilla en función de la finalidad del tratamiento.

En su Dictamen sobre la publicidad comportamental, el Grupo de trabajo concluyó lo siguiente: «…parece de capital importancia que los buscadores dispongan de la configuración de «no aceptación y no transmisión de cookies de terceros». Para complementar esto y hacerlo más eficaz, los buscadores deben pedir a los usuarios que entren en un asistente de privacidad la primera vez que instalen o actualicen el buscador y proporcionarles un método fácil de ejercer su opción durante la utilización del producto»[46].

III.B.5. Artículo 6, apartado 3, artículo 9, apartados 3 y 4, - posibilidad de retirar el consentimiento

«… posibilidad de retirar su consentimiento … en cualquier momento …»

La posibilidad de retirar el consentimiento, que está implícita en la Directiva 95/46/CE, se recoge en diversas disposiciones de la Directiva sobre privacidad. Así se declaró

[45] Dictamen 5/2004 sobre comunicaciones no solicitadas con fines de venta directa con arreglo al artículo 13 de la Directiva 2002/58/CE, adoptado el 27.2.2004.

[46] Dictamen de 22.6.2010 WP 171, op.cit.

explícitamente en el Dictamen del Grupo de trabajo sobre el uso de los datos de localización con vistas a prestar servicios con valor añadido[47]:

« En virtud de lo dispuesto en el artículo 9 de la Directiva 2002/58/CE, las personas que hayan dado su consentimiento para el tratamiento de datos de localización distintos de los datos de tráfico podrán retirar dicho consentimiento en cualquier momento y deberán gozar de la posibilidad, a través de un medio simple y gratuito, de oponerse temporalmente al tratamiento de tales datos. El Grupo considera que estos derechos, que pueden consistir en la aplicación del derecho a oponerse al tratamiento de los datos de localización, son esenciales dado el carácter sensible de los mismos. El Grupo está convencido de que una condición previa para el ejercicio de estos derechos es que se mantenga informadas a las personas, no sólo cuando se abonan a un servicio sino también cuando lo usan. Cuando un servicio requiere el tratamiento permanente de datos de localización, el Grupo estima que el proveedor del servicio debería recordar regularmente a la persona de que se trate que su equipo terminal ha sido, será o puede ser localizado. Ello le permitirá, si así lo desea, ejercer el derecho a retirar su consentimiento con arreglo a lo dispuesto en el artículo 9 de la Directiva 2002/58/CE.»

Como ya se ha mencionado anteriormente, esto implica que la retirada afectará al futuro y no al tratamiento de datos realizado en el pasado durante el periodo en que los datos se recopilaron legalmente. Por lo tanto, las decisiones o tratamientos realizados previamente sobre la base de esta información no pueden anularse sin más. Ahora bien, si no existe ningún otro fundamente jurídico para proseguir almacenando datos, el responsable del tratamiento debe suprimirlos.

IV. Conclusiones

El presente dictamen examina el marco jurídico que regula el uso del consentimiento con arreglo a la Directiva 95/46/CE y la Directiva 2002/58/CE. Este ejercicio tiene un doble objetivo: en primer lugar, clarificar los requisitos jurídicos existentes y explicar cómo se aplican en la práctica. Al mismo tiempo se plantea si el marco existente sigue siendo el adecuado a la luz de las numerosas formas nuevas de tratamiento de datos personales, así como la necesidad de modificarlo.

IV.1. Aclaración de los aspectos clave del marco actual

El artículo 2, letra h), de la Directiva 95/46/CE define el consentimiento como «toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan». El artículo 7 de la Directiva, que establece la base jurídica del tratamiento de datos personales, dispone que el consentimiento «inequívoco» es uno de sus requisitos jurídicos. El artículo 8 establece el requisito jurídico de que el consentimiento sea «explícito» para tratar datos sensibles. El artículo 26, apartado 1, de la Directiva 95/46/CE y diversas disposiciones de la Directiva sobre privacidad exigen que exista consentimiento para realizar determinadas actividades específicas de tratamiento de datos en el ámbito de su aplicación. Los puntos desarrollados en este dictamen pretenden clarificar los diversos elementos del marco legal a fin de facilitar su aplicación por todas las partes interesadas.

47 Dictamen 5/2005 sobre el uso de los datos de localización con vistas a prestar servicios con valor añadido, adoptado el 25.11.2005 (WP 115).

Elementos y observaciones de carácter general

- El consentimiento es uno de los seis fundamentos jurídicos del tratamiento de datos personales (uno de los cinco en el caso de datos sensibles); es un fundamento importante que permite al interesado cierto control sobre el tratamiento de sus datos; La importancia del consentimiento para afirmar la autonomía y autodeterminación de la persona depende de que se use en un contexto adecuado y reúna los elementos necesarios.

- Generalmente, el marco jurídico de la Directiva 95/46/CE se aplica siempre que se requiere el consentimiento, ya sea en línea o fuera de línea. Por ejemplo, al vendedor de ladrillos y mortero que exige la firma en un formulario de papel para solicitar una tarjeta de fidelidad se le aplican las mismas normas que si lo hiciera a través de un sitio de Internet. La Directiva sobre privacidad también especifica algunas operaciones de tratamiento de datos que requieren consentimiento: la mayoría se refiere al tratamiento de datos en relación con la prestación de servicios de comunicaciones electrónicas disponibles al público. Los requisitos de validez del consentimiento que establece la Directiva 2000/58/CE son los mismos de la Directiva 95/46/CE.

- Las situaciones en que los responsables utilizan el consentimiento como un fundamento jurídico del tratamiento de datos personales no deberían confundirse con aquellas en que el responsable basa el tratamiento en otros fundamentos jurídicos que implican un derecho de objeción individual. Por ejemplo, puede ser el caso de un tratamiento basado en los «legítimos intereses» del responsable del tratamiento según el antiguo artículo 7, letra f), de la Directiva 95/46/CE, pero al que la persona tiene derecho a oponerse con arreglo al artículo 14, letra a), de dicha Directiva. Otro ejemplo es el del responsable que envía comunicaciones electrónicas a los clientes para promocionar sus propios productos o servicios u otros similares, a lo que no obstante, las personas pueden oponerse con arreglo al artículo 13, apartado 2, de la Directiva 2002/58/CE. En ambos casos los interesados tienen derecho a oponerse al tratamiento, algo distinto del consentimiento.

- La utilización del consentimiento para tratar datos personales no exime al responsable de la obligación de cumplir otros requisitos previstos en el marco jurídico de protección de datos como, por ejemplo, el respeto del principio de proporcionalidad previsto en el artículo 6, apartado 1, letra c), la seguridad del tratamiento previsto en el antiguo artículo 17, etc.

- El consentimiento válido presupone la capacidad de la persona para darlo. Las normas que regulan la capacidad para consentir no están armonizadas y pueden variar de un Estado miembro a otro.

- Las personas que han dado su consentimiento deberían tener la posibilidad de retirarlo para evitar que sus datos se sigan tratando. Esto se confirma también en la Directiva sobre privacidad en lo que respecta a las operaciones de tratamiento de datos específicos basadas en el consentimiento, como el tratamiento de datos de localización distintos de los datos de tráfico.

- El consentimiento debe darse antes del comienzo del tratamiento de datos personales, pero también puede requerirse durante el tratamiento, cuando surja una finalidad nueva. Así se subraya en diversas disposiciones de la Directiva

2002/58/CE, mediante el requisito «antes de» (artículo 6, apartado 3) o en el texto de las disposiciones (artículo 5, apartado 3).

Elementos específicos del marco jurídico relacionados con el consentimiento

- Para ser válido, el consentimiento debe ser [una manifestación de voluntad] «libre». Es decir, no debe haber ningún riesgo de engaño, intimidación o consecuencias negativas significativas para el interesado en caso de que no consienta. Las operaciones de tratamiento de datos en el ámbito laboral, donde existe un elemento de subordinación, así como en los servicios de la administración como la salud, pueden exigir una evaluación particularmente atenta de la libertad de la persona para dar su consentimiento.

- El consentimiento debe ser «específico». El consentimiento indiscriminado sin indicación de los fines exactos no se ajusta a la norma. Más que insertar la información en las condiciones generales del contrato, es necesario utilizar cláusulas de consentimiento específicas, separadas de las condiciones y reglas generales.

- El consentimiento debe estar «informado». Los artículos 10 y 11 de la Directiva enumeran el tipo de información que debe suministrarse necesariamente a las personas. En cualquier caso, la información suministrada debe ser suficiente para garantizar que los individuos puedan adoptar decisiones bien informadas sobre el tratamiento de sus datos personales. La necesidad de que el consentimiento esté «informado» se traduce en dos requisitos adicionales. En primer lugar, la manera de suministrar información debe garantizar el uso de un lenguaje adecuado que permita al interesado entender lo que está consintiendo y las finalidades. Hay que tener en cuenta el contexto. La utilización de una jerga técnica o jurídica demasiado complicada no cumple los requisitos de la ley. En segundo lugar, la información a los usuarios debería ser clara y suficientemente llamativa para que los usuarios no la puedan pasar por alto. La información debe suministrarse directamente a las personas. No basta con ponerla disposición en algún sitio.

- En cuanto a cómo debe darse el consentimiento, el artículo 8, apartado 2, letra a), exige un consentimiento «explícito» para tratar datos sensibles, lo que significa una respuesta activa, verbal o escrita, por la que la persona manifiesta su deseo de que sus datos se traten para determinados fines.   Por tanto, el consentimiento expreso no puede obtenerse por medio de una casilla preseleccionada. El interesado debe realizar alguna acción positiva que indique su consentimiento y debe tener la libertad de no consentir.

- En cuanto a los datos no sensibles, el artículo 7, letra a), exige que el consentimiento sea «inequívoco». Este término implica la utilización de mecanismos para obtener el consentimiento que no dejen lugar a dudas sobre la intención de la persona al dar su consentimiento. En la práctica, este requisito permite a los responsables utilizar diferentes tipos de mecanismos para obtener el consentimiento, que van desde declaraciones que indiquen acuerdo (consentimiento expreso) hasta mecanismos basados en acciones dirigidas a indicar acuerdo.

- Por lo general, el consentimiento basado en la inacción o el silencio de la persona no constituye un consentimiento válido, especialmente en el contexto en línea. Este problema se plantea especialmente cuando se utilizan parámetros de aceptación por defecto que el interesado debe modificar si desea rechazar el tratamiento. Así sucede, por ejemplo, al utilizar las casillas preseleccionadas o los parámetros del navegador de Internet seleccionados por defecto para recopilar datos.

IV. 2 Evaluación del marco actual y posible necesidad de cambio

Evaluación global

El Grupo de trabajo considera que el actual marco de protección de datos contiene un conjunto de normas bien concebidas que establecen las condiciones de validez del consentimiento a efectos de legitimar las operaciones de tratamiento de datos. Estas normas se aplican tanto en entornos en línea como fuera de línea. Concretamente:

El marco actual equilibra con éxito los diversos aspectos de interés. Por una parte, establece que sólo es válido el consentimiento auténtico e informado. A este respecto, resulta pertinente y satisfactorio el artículo 2, letra h), que exige explícitamente que el consentimiento sea libre, específico e informado. Por otra parte, este requisito no constituye ningún corsé sino más bien aporta flexibilidad y evita reglas tecnológicas específicas. Así queda ilustrado en el mismo artículo 2, letra h), que define el consentimiento como toda manifestación de voluntad del interesado. Esto proporciona un margen suficiente en cuanto a las maneras de manifestación de la voluntad. Los artículos 7 y 8, que requieren que el consentimiento sea inequívoco y explícito, respectivamente, han captado bien la necesidad de equilibrio entre ambos aspectos, al proporcionar flexibilidad y evitar estructuras demasiado rígidas al mismo tiempo que garantizan la protección.

El resultado es un marco que, si se aplica y ejecuta adecuadamente, puede seguir el ritmo de evolución de la gran variedad de operaciones de tratamiento de datos que surgen como consecuencia del desarrollo tecnológico.

No obstante, no siempre es fácil determinar en la práctica cuándo es necesario el consentimiento y, en particular, los requisitos de su validez, así como la manera en que deben aplicarse, habida cuenta de la falta de uniformidad entre los Estados miembros. La aplicación a nivel nacional ha dado lugar a diversos enfoques. Más adelante se describen las deficiencias específicas que se señalaron en los debates del Grupo del artículo 29 que condujeron a la adopción del presente dictamen.

Cambios posibles

- La noción de consentimiento inequívoco es útil porque establece un sistema no demasiado rígido que ofrece una alta protección. Podría conducir a un sistema razonable, pero lamentablemente su significado se malinterpreta o sencillamente se ignora. Si bien las indicaciones y ejemplos desarrollados anteriormente deberían contribuir a mejorar la seguridad jurídica y la protección de los derechos individuales cuando se utiliza el consentimiento como base jurídica, parece que la situación requiere algunos cambios.
- En particular, el Grupo del artículo 29 considera que la propia redacción («inequívoca») mejoraría si se clarificara más en el marco de la revisión del marco general de la protección de datos. La clarificación debería subrayar que el consentimiento inequívoco exige utilizar mecanismos que no dejen lugar a dudas sobre la intención de consentir del interesado. Al mismo tiempo habría que aclarar que la utilización de opciones por defecto que el interesado debe modificar para

negarse al tratamiento (consentimiento basado en el silencio) no constituye consentimiento inequívoco. Así sucede sobre todo en el contexto en línea.

- Además de la clarificación mencionada, el Grupo del artículo 29 propone:

    i. *En primer lugar,* incluir en la definición de consentimiento del artículo 2, letra h), la palabra «inequívoca» (o equivalente), a fin de reforzar la noción de que sólo el consentimiento basado en declaraciones o acciones que indiquen acuerdo constituye un consentimiento válido. Además de clarificar, así se adaptaría el concepto de consentimiento del artículo 2, letra h) a los requisitos de validez del consentimiento del artículo 7. Por otra parte, el significado de la palabra «inequívoca» podría explicarse más en un considerando del futuro marco jurídico.

    ii. *En segundo lugar,* en el contexto de la obligación de responsabilidad general, los responsables deberían estar en condiciones de demostrar que han obtenido el consentimiento. De hecho, si la carga de la prueba se refuerza obligando a los responsables a demostrar que han obtenido efectivamente el consentimiento del interesado, estos deberán aplicar prácticas y mecanismos normalizados para obtener y demostrar el consentimiento inequívoco. El tipo de mecanismo dependerá del contexto y deberá tener en cuenta los hechos y circunstancias del tratamiento, así como sus riesgos particulares.

- El Grupo del artículo 29 no está convencido de que el marco legal deba exigir el consentimiento explícito como norma general para todos los tipos de operaciones de tratamiento, incluidas las reguladas actualmente por el artículo 7 de la Directiva. Considera que la norma exigible debería seguir siendo el consentimiento inequívoco que abarca tanto el consentimiento explícito como el derivado de «acciones» inequívocas. Esta opción ofrece más flexibilidad a los responsables para obtener el consentimiento y puede dar lugar a un procedimiento global más rápido y de fácil aplicación.

- Algunos aspectos del marco jurídico que se aplican al consentimiento proceden de los textos o antecedentes jurídicos, o bien se han desarrollado a través de la jurisprudencia y los dictámenes del Grupo del artículo 29. Para mayor seguridad jurídica, estos aspectos deberían incorporarse expresamente al nuevo marco legislativo de la protección de datos. Podrían considerarse los puntos siguientes:

    i. Inclusión de una cláusula expresa que establezca el derecho de la persona a retirar su consentimiento.

    ii. Reforzar la noción de que el consentimiento debe darse antes del comienzo del tratamiento, o antes de cualquier nuevo uso de los datos para fines no incluidos en el consentimiento inicial, cuando no exista ningún otro fundamento jurídico del tratamiento.

    iii. Incluir los requisitos explícitos relativos a la calidad (obligación de suministrar información sobre el tratamiento de datos de forma fácil de entender, en un lenguaje claro y sencillo) y la accesibilidad de la información (obligación de que la información sea llamativa, destacada y directamente accesible). Esto es de vital importancia para que las personas puedan decidir con conocimiento de causa.

- Por último, con respecto a las personas que carecen de capacidad jurídica, podrían preverse disposiciones para garantizar una mayor protección, que incluyan:

    i. Aclaración de las circunstancias en que se requiere el consentimiento de los padres o representantes de la persona sin capacidad, incluido el límite de edad por debajo del cual este consentimiento sería obligatorio.

    ii. Establecer la obligación de utilizar mecanismos de comprobación de la edad que pueden variar según circunstancias como la edad de los niños, el tipo de tratamiento, ya sea de especial riesgo, ya sea que la información la conserve el responsable o la ponga a disposición de terceros;

    iii. Requisito de adaptar la información a los niños para que puedan entender lo que significa la recogida de sus datos y puedan dar su consentimiento;

    iv. Garantías específicas que identifiquen determinadas actividades de tratamiento como la publicidad comportamental, en las que el consentimiento no debería ser la base para legitimar el tratamiento de datos personales.

El Grupo del artículo 29 volverá a ocuparse del tema del consentimiento. En particular, las autoridades nacionales de protección de datos y el Grupo de trabajo podrán decidir en una fase posterior elaborar directrices para desarrollar en mayor medida el presente dictamen mediante ejemplos prácticos adicionales relativos a la utilización del consentimiento.

Bruselas, 13 de julio de 2011

Por el Grupo de trabajo

Presidente
Jacob KOHNSTAMM