



**00264/10/ES
WP 169**

Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento»

Adoptado el 16 de febrero de 2010

Este Grupo se creó en virtud del artículo 29 de la Directiva 95/46/CE. Se trata de 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.

La secretaría la facilita la Dirección D (Derecho Fundamentales y Ciudadanía) de la Dirección General de Justicia, Libertad y Seguridad de la Comisión Europea, B-1049 Bruselas, Bélgica, despacho LX-46 01/190.

Sitio web: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

ÍNDICE

Resumen	1
I. Introducción	2
II. Observaciones generales y cuestiones políticas	3
II.1. Papel de los conceptos	4
II.2. Contexto pertinente.....	6
II.3. Algunos desafíos fundamentales	7
III. Análisis de las definiciones	8
III.1. Definición de responsable del tratamiento	8
III.1.a) Elemento preliminar: «determine»	9
III.1.b) Tercer elemento: «fines y medios del tratamiento».....	13
III.1.c) Primer elemento: «persona física o jurídica o cualquier otro organismo»	16
III.1.d) Segundo elemento: «solo o conjuntamente con otros».....	19
III.2. Definición del encargado del tratamiento.....	27
III.3. Definición de tercero	34
IV. Conclusiones.....	35

Resumen

El concepto de «responsable del tratamiento» y su interacción con el concepto de «encargado del tratamiento» desempeñan un papel fundamental en la aplicación de la Directiva 95/46/CE, puesto que determinan quién debe ser responsable del cumplimiento de las normas de protección de datos, cómo pueden ejercer sus derechos los interesados, cuál es la legislación nacional aplicable y con qué eficacia pueden operar las autoridades de protección de datos.

Las diferencias de organización en los sectores público y privado, el desarrollo de las TIC y la globalización del tratamiento de datos aumentan la complejidad de dicho tratamiento y requieren una aclaración de estos conceptos con objeto de garantizar una aplicación eficaz y el cumplimiento en la práctica.

El concepto de responsable del tratamiento es autónomo, en el sentido de que debe interpretarse fundamentalmente con arreglo a la legislación comunitaria de protección de datos, y funcional, en el sentido de que su objetivo es asignar responsabilidades en función de la capacidad de influencia de hecho, y, por consiguiente, se basa en un análisis de los hechos más que en un análisis formal.

La definición de la Directiva consta de tres componentes fundamentales:

- el aspecto personal (*«la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo»*);
- la posibilidad de un control plural (*«que solo o conjuntamente con otros»*); y
- los elementos esenciales para distinguir al responsable del tratamiento de otros agentes (*«determine los fines y los medios del tratamiento de datos personales»*)

El análisis de estos componentes lleva a una serie de conclusiones que se resumen en el apartado IV del dictamen.

Este dictamen analiza también el concepto de encargado del tratamiento, cuya existencia depende de una decisión adoptada por el responsable del tratamiento, que puede decidir que los datos se traten dentro de su organización o bien delegar todas o una parte de las actividades de tratamiento en una organización externa. Para poder actuar como encargado del tratamiento tienen que darse dos condiciones básicas: por una parte, ser una entidad jurídica independiente del responsable del tratamiento y, por otra, realizar el tratamiento de datos personales por cuenta de éste.

El Grupo reconoce las dificultades para poner en práctica las definiciones de la Directiva en un entorno complejo en el que caben muchas situaciones hipotéticas que impliquen la actuación de responsables y encargados del tratamiento, solos o conjuntamente, y con distintos grados de autonomía y responsabilidad.

En su análisis hace hincapié en la necesidad de asignar la responsabilidad de tal manera que el cumplimiento de las normas de protección de datos se vea suficientemente garantizado en la práctica. Con todo, no ha encontrado razón alguna para considerar que la distinción actual entre responsables y encargados del tratamiento ya no sea pertinente y viable desde esta perspectiva.

Por ello, el Grupo espera que las explicaciones dadas en su dictamen, ilustradas con ejemplos concretos tomados de la experiencia cotidiana de las autoridades de protección de datos, sirvan de orientación sobre cómo interpretar estas definiciones esenciales de la Directiva.

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,

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

Visto su Reglamento interno,

Ha adoptado el siguiente dictamen:

I. Introducción

El concepto de «responsable del tratamiento» y su interacción con el concepto de «encargado del tratamiento» desempeñan un papel fundamental en la aplicación de la Directiva 95/46/CE, puesto que determinan quién debe ser responsable del cumplimiento de las normas de protección de datos y la manera en que los interesados pueden ejercer sus derechos en la práctica. El concepto de responsable del tratamiento de datos también es esencial a la hora de determinar la legislación nacional aplicable y para el ejercicio eficaz de las tareas de supervisión conferidas a las autoridades de protección de datos.

Por ello, es de suma importancia que el significado preciso de estos conceptos y los criterios para su uso correcto sean suficientemente claros y sean compartidos por todas aquellas personas en los Estados miembros que desempeñan un papel en la aplicación de la Directiva y en la aplicación, evaluación y ejecución de las disposiciones nacionales por las que surte efecto.

Hay indicios de que puede haber una falta de claridad, al menos en lo concerniente a determinados aspectos de estos conceptos, y algunos puntos de vista divergentes entre las personas competentes en los distintos Estados miembros que pueden dar lugar a interpretaciones diferentes de los mismos principios y definiciones introducidos a efectos de la armonización a nivel europeo. Por este motivo, el Grupo del Artículo 29 ha decidido, como parte de su programa de trabajo estratégico para 2008-2009, prestar especial atención a la elaboración de un documento que exponga un enfoque común de estas cuestiones.

El Grupo reconoce que la aplicación concreta de los conceptos de responsable del tratamiento de datos y encargado del tratamiento de datos se está haciendo cada vez más compleja. Esto se debe ante todo a la creciente complejidad del entorno en el que se usan estos conceptos y, en particular, a una tendencia en aumento, tanto en el sector privado como en el público, hacia una diferenciación organizativa, combinada con el desarrollo de las TIC y la globalización, lo cual puede dar lugar a que se planteen cuestiones nuevas y difíciles y a que, en ocasiones, se vea disminuido el nivel de protección de los interesados.

A pesar de que las disposiciones de la Directiva se formularon de un modo tecnológicamente neutro y hasta el momento han resistido bien en un contexto en constante evolución, estas complejidades pueden generar, de hecho, incertidumbres en cuanto a la asignación de responsabilidades y al alcance de las legislaciones nacionales aplicables. Estas incertidumbres pueden tener un efecto negativo sobre el cumplimiento de las normas de protección de datos en áreas críticas y sobre la eficacia de la legislación sobre protección de datos en su conjunto. El Grupo ya ha abordado algunos de estos asuntos en relación con determinadas cuestiones específicas¹, pero considera que ahora es necesario brindar unas directrices más desarrolladas y una orientación específica a fin de garantizar un enfoque coherente y armonizado.

En consecuencia, el Grupo ha decidido ofrecer en este dictamen —de manera similar a lo que hizo en su dictamen sobre el concepto de datos personales²— algunas aclaraciones y ejemplos concretos³ respecto de los conceptos de responsable del tratamiento de datos y encargado del tratamiento de datos.

II. Observaciones generales y cuestiones políticas

La Directiva hace referencia explícita al concepto de responsable del tratamiento en varias de sus disposiciones. Las definiciones de «responsable del tratamiento» y «encargado del tratamiento» en el artículo 2, letras d) y e), de la Directiva 95/46/CE (en lo sucesivo denominada «la Directiva») rezan así:

«responsable del tratamiento»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que solo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales; en caso de que los fines y los medios del tratamiento estén determinados por disposiciones legislativas o reglamentarias nacionales o comunitarias, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el Derecho nacional o comunitario;

«encargado del tratamiento»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que trate datos personales por cuenta del responsable del tratamiento.

Estas definiciones se perfilaron durante las negociaciones del proyecto de propuesta de Directiva a principios de los años 90, y el concepto de «responsable del tratamiento» se tomó básicamente del Convenio 108 del Consejo de Europa firmado en 1981. Durante dichas negociaciones se produjeron algunos cambios importantes.

En primer lugar, «autoridad controladora del fichero» del Convenio 108 se sustituyó por «responsable del tratamiento» en referencia al «tratamiento de datos personales». Se trata de una noción amplia, definida en el artículo 2, letra b), de la Directiva como «cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos

¹ Véase, por ejemplo, el Dictamen 10/2006 sobre el tratamiento de datos personales por parte de la Sociedad de Telecomunicaciones Financieras Interbancarias Mundiales (Society for Worldwide Interbank Financial Telecommunication – SWIFT), adoptado el 22 de noviembre de 2006 (WP 128) y, más recientemente, el Dictamen 5/2009 sobre las redes sociales en línea, adoptado el 12 de junio de 2009 (WP 163).

² Dictamen 4/2007 sobre el concepto de datos personales, adoptado el 20 de junio de 2007 (WP 136).

³ Los ejemplos se basan en la práctica nacional o europea corriente y pueden haberse modificado o revisado en aras de su mejor comprensión.

automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción». Por lo tanto, el concepto de «responsable del tratamiento» ya no se empleaba para un objeto estático («el fichero»), sino en relación con actividades que reflejaban el ciclo de vida de la información desde su recogida hasta su destrucción, y esto requería tanto un examen en detalle como de conjunto («operación o conjunto de operaciones»). Aunque el resultado haya podido ser en muchos casos el mismo, al concepto se le confería así un significado y alcance mucho más amplios y dinámicos.

Otros cambios implicaban la introducción de la posibilidad de un «control plural» («solo o conjuntamente con otros»), la exigencia de que el responsable del tratamiento «determine los fines y los medios del tratamiento de datos personales» y la noción de que tal determinación podía hacerse con arreglo a la legislación nacional o comunitaria o por otros medios. La Directiva introduce asimismo el concepto de «encargado del tratamiento», que no se menciona en el Convenio 108. Estos y otros cambios se analizarán con más detalle a lo largo del presente dictamen.

II.1. Papel de los conceptos

Mientras el concepto de responsable del tratamiento (autoridad controladora del fichero) desempeña un papel muy limitado⁴ en el Convenio 108, la situación es completamente distinta en la Directiva. El artículo 6, apartado 2, establece explícitamente que «corresponderá a los responsables del tratamiento garantizar el cumplimiento de lo dispuesto en el apartado 1». Esto remite a los principios fundamentales relativos a la calidad de los datos, entre otros el principio enunciado en el artículo 6, apartado 1, letra a) de que «los datos personales sean [...] tratados de manera leal y lícita». Esto significa de hecho que todas las disposiciones que establecen condiciones para el tratamiento lícito se dirigen esencialmente al responsable del tratamiento, aunque esto no siempre se formule con claridad.

Por lo demás, las disposiciones relativas a los derechos de los interesados a la información, al acceso, a la rectificación, a la supresión y al bloqueo y al derecho de oposición al tratamiento de datos personales (artículos 10 a 12 y 14) se han formulado de tal manera que implican la creación de obligaciones para el responsable del tratamiento. El responsable del tratamiento también está en el centro de las disposiciones sobre notificación y controles previos (artículos 18 a 21). Por último, no es sorprendente que el responsable del tratamiento también deba responder, en principio, del perjuicio resultante de un tratamiento ilícito (artículo 23).

Esto significa que el papel primero y primordial del concepto de responsable del tratamiento es determinar quién debe asumir la responsabilidad del cumplimiento de las normas sobre protección de datos y de qué manera los interesados pueden ejercer sus derechos en la práctica⁵. En otras palabras, debe asignar la responsabilidad.

⁴ No figura en ninguna de las disposiciones sustantivas, excepto en el artículo 8, letra a), en relación con el derecho a ser informado (principio de transparencia). El responsable del tratamiento en tanto que parte responsable sólo tiene visibilidad en ciertas partes de la exposición de motivos.

⁵ Véase también el considerando 25 de la Directiva 95/46/CE: «Considerando que los principios de la protección tienen su expresión, por una parte, en las distintas obligaciones que incumben a las personas, autoridades públicas, empresas, agencias u otros organismos que efectúen tratamientos — obligaciones relativas, en particular, a la calidad de los datos, la seguridad técnica, la notificación a las autoridades de control y las circunstancias en las que se puede efectuar el tratamiento— y, por otra

Esto apunta al núcleo mismo de la Directiva, cuyo primer objetivo es la «protección de las personas en lo que respecta al tratamiento de datos personales». Este objetivo sólo puede alcanzarse y ponerse en práctica si a los responsables del tratamiento de datos se les ofrecen los estímulos suficientes, por medios legales y de otro tipo, para que adopten todas las medidas necesarias a fin de garantizar que esta protección se dé en la práctica. Esto se ve confirmado por el artículo 17, apartado 1, de la Directiva, que establece *«la obligación del responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales»*.

Los medios para estimular la responsabilidad pueden ser proactivos o reactivos. En el primer caso, consisten en garantizar la aplicación efectiva de las medidas de protección de datos y unos medios suficientes para que los responsables del tratamiento puedan rendir cuentas de su actividad. En el segundo caso, los medios pueden abarcar la responsabilidad civil y sanciones para garantizar que se indemnicen los perjuicios de cierta consideración y se adopten las medidas pertinentes para subsanar posibles errores o irregularidades.

El concepto de responsable del tratamiento también es un elemento esencial para determinar qué legislación nacional es aplicable a una operación o conjunto de operaciones de tratamiento de datos. La principal norma sobre el Derecho aplicable con arreglo al artículo 4, apartado 1, letra a), de la Directiva es que los Estados miembros aplican sus disposiciones nacionales *«a todo tratamiento de datos personales cuando [...] sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento en el territorio del Estado miembro»*. Esta disposición continúa así: *«cuando el mismo responsable del tratamiento esté establecido en el territorio de varios Estados miembros deberá adoptar las medidas necesarias para garantizar que cada uno de dichos establecimientos cumple las obligaciones previstas por el Derecho nacional aplicable»*. Esto significa que el o los establecimientos del responsable del tratamiento también determinan la o las legislaciones nacionales aplicables, y posiblemente un cierto número de legislaciones nacionales diferentes aplicables, y la manera en que se relacionan entre sí⁶.

Por último, hay que señalar que el concepto de responsable del tratamiento aparece en muchas disposiciones de la Directiva como un elemento del alcance de tales disposiciones o de una condición específica aplicable en virtud de ellas; por ejemplo, el artículo 7 establece que el tratamiento de datos personales sólo puede efectuarse si: *«c) es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento, e) es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos, o f) es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el*

parte, en los derechos otorgados a las personas cuyos datos sean objeto de tratamiento de ser informadas acerca de dicho tratamiento, de poder acceder a los datos, de poder solicitar su rectificación o incluso de oponerse a su tratamiento en determinadas circunstancias».

⁶ El Grupo tiene previsto adoptar también un dictamen sobre el «Derecho aplicable» a lo largo de 2010. Cuando las instituciones y órganos comunitarios tratan datos personales, la evaluación de la responsabilidad también es pertinente en relación con la posible aplicación del Reglamento (CE) 45/2001 u otros instrumentos jurídicos de la UE pertinentes.

tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés...». La identidad del responsable del tratamiento también es un elemento importante de la información al interesado que se exige con arreglo a los artículos 10 y 11.

El concepto de «encargado del tratamiento» desempeña un papel importante en el contexto de la confidencialidad y seguridad del tratamiento (artículos 16 y 17), dado que sirve para determinar las responsabilidades de quienes están más estrechamente vinculados al tratamiento de datos personales, ya sea bajo la autoridad directa del responsable del tratamiento o por cuenta de éste. La distinción entre «responsable del tratamiento» y «encargado del tratamiento» sirve primordialmente para diferenciar entre quienes asumen la responsabilidad en tanto que responsables y quienes sólo actúan por cuenta de éstos. De nuevo, se trata básicamente de cómo asignar la responsabilidad. De ello pueden derivarse otras consecuencias, ya sea en lo relativo a la legislación aplicable o a otras cuestiones.

Con todo, en el caso del encargado del tratamiento hay una consecuencia adicional — tanto para el responsable como para el encargado— que se deriva del hecho de que, con arreglo al artículo 17 de la Directiva, la legislación aplicable para la seguridad del tratamiento debe ser la del Estado miembro en el que esté establecido el encargado⁷.

Por último, según la definición del artículo 2, letra f): *«"tercero": la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento»*. Por lo tanto, el responsable y el encargado y su personal respectivo se consideran el «círculo restringido del tratamiento de datos» y no están cubiertos por disposiciones especiales relativas a terceros.

II.2. Contexto pertinente

Unas evoluciones divergentes en el contexto pertinente han llevado a que estos asuntos sean más urgentes y también más complejos que antes. En el momento de la firma del Convenio 108, y en buena medida también cuando se adoptó la Directiva 96/46/CE, el ámbito del tratamiento de datos aún era relativamente claro y sencillo, pero éste ya no es el caso.

Esto se debe, en primer lugar, a una tendencia creciente hacia la diferenciación organizativa en la mayoría de los sectores implicados. En el sector privado, la distribución de riesgos financieros y de otro tipo ha llevado a la actual diversificación empresarial, que aún se ve acentuada por las fusiones y adquisiciones. En el sector público, se está produciendo una diferenciación similar en el contexto de la descentralización o separación de los departamentos que elaboran las políticas y agencias ejecutivas competentes. En ambos sectores se pone un énfasis cada vez mayor en el desarrollo de cadenas de prestación de servicios entre organizaciones y en el recurso a la subcontratación o externalización de servicios para aprovechar la especialización y posibles economías de escala. Como consecuencia de ello se ha producido un incremento de determinados servicios ofrecidos por prestatarios que no siempre consideran que sean responsables o deban rendir cuentas. Debido a las opciones organizativas de las empresas

⁷ Véase el artículo 17, apartado 3, segundo guión: «las obligaciones [...] tal como las define la legislación del Estado miembro en el que esté establecido el encargado, incumben también a éste».

(y de sus contratistas o subcontratistas), las bases de datos correspondientes pueden encontrarse en uno o varios países dentro o fuera de la Unión Europea.

El desarrollo de las tecnologías de la información y la comunicación («TIC») ha facilitado en gran medida estos cambios en la organización y al mismo tiempo ha añadido, por su parte, algunos cambios. Las responsabilidades a distintos niveles —que a menudo son el resultado de diferencias de organización— por lo común requieren e incitan al uso intensivo de TIC. El desarrollo y despliegue de productos y servicios TIC también dan lugar a nuevas funciones y responsabilidades por derecho propio que no siempre interactúan de forma clara con las responsabilidades existentes o que se están desarrollando en las organizaciones clientes. Por ello es importante tener conciencia de las diferencias pertinentes y aclarar las responsabilidades cuando sea necesario. La introducción de la microtecnología —como chips RFID en productos de consumo— plantea cuestiones similares sobre el desplazamiento de las responsabilidades. En el otro extremo han surgido cuestiones nuevas y complejas relacionadas con el uso de la informática distribuida, en particular la «computación en la nube» y la «informática en malla (*grid*)»⁸.

La globalización es otro factor de complicación. Cuando la diferenciación organizativa y el desarrollo de las TIC implican múltiples jurisdicciones, como ocurre a menudo en asuntos relacionados con internet, es más que probable que se planteen cuestiones relativas al Derecho aplicable, no sólo en la UE o en el EEE, sino también respecto de terceros países. Un ejemplo ilustrativo de esto se encuentra en el ámbito de la lucha contra el dopaje: la Agencia Mundial Antidopaje (AMA), con sede en Suiza, trabaja con una base de datos que contiene información sobre atletas (ADAMS) y que se gestiona desde Canadá, en cooperación con las organizaciones nacionales antidopaje de todo el mundo. El WP29 ha destacado la división y atribución de responsabilidades como elementos que plantean dificultades específicas⁹.

Esto significa que las cuestiones centrales que se abordan en el presente dictamen tienen una gran relevancia práctica y pueden tener importantes consecuencias.

II.3. Algunos desafíos fundamentales

Desde la óptica de los objetivos de la Directiva, es de suma importancia garantizar que la responsabilidad del tratamiento de datos se defina con claridad y pueda aplicarse de forma efectiva.

Si no está lo suficientemente claro qué es lo que se exige y a quién —por ejemplo, nadie es responsable o son varios los responsables posibles del tratamiento—, hay un riesgo evidente de que poco o nada ocurra y las disposiciones legales resulten ineficaces. También es posible que las ambigüedades en la interpretación desemboquen en pretensiones contrapuestas y en otras controversias, en cuyo caso los efectos positivos

⁸ La «computación en la nube» es un tipo de informática en el que se proporcionan capacidades de TI escalables y elásticas en forma de servicio a un conjunto de usuarios de tecnologías de internet. Los servicios de computación en la nube consisten por lo común en proporcionar aplicaciones empresariales habituales en línea a las que se accede desde un navegador web, mientras que el *software* y los datos están almacenados en servidores. En este sentido, la nube no es una isla, sino un elemento de conexión global de la información y los usuarios en todo el mundo. En cuanto a la «informática basada en la GRID», véase el ejemplo 19.

⁹ Dictamen 3/2008 de 1 de agosto de 2008 sobre el proyecto de norma internacional del Código Mundial Antidopaje para la protección de la intimidad (WPI 56).

serían menores de lo esperado o podrían verse mermados o contrarrestados por consecuencias negativas imprevistas.

En todos estos casos el desafío principal es, por tanto, proporcionar la suficiente claridad para permitir y garantizar una aplicación eficaz y el cumplimiento en la práctica. En caso de duda, debería privilegiarse la solución con mayores probabilidades de surtir tales efectos.

Con todo, los mismos criterios que brindan la claridad necesaria también podrían dar lugar a una mayor complejidad y a consecuencias indeseadas. Por ejemplo, la diferenciación del control, en consonancia con las realidades de organización, puede aumentar la complejidad en lo relativo al Derecho nacional aplicable cuando estén implicadas distintas jurisdicciones.

Por lo tanto, el análisis debería prestar especial atención a la diferencia entre consecuencias aceptables en el marco de las normas vigentes y la necesidad de ajustar en su caso tales normas para garantizar que sigan surtiendo efecto y evitar consecuencias indebidas en circunstancias cambiantes.

Esto significa que el presente análisis es de gran importancia estratégica y debería aplicarse con cautela y plena conciencia de la posible interrelación entre diferentes asuntos.

III. Análisis de las definiciones

III.1. Definición de responsable del tratamiento

La definición de responsable del tratamiento en la Directiva consta de tres componentes fundamentales que, a efectos del presente dictamen, se analizarán por separado. Se trata de los siguientes:

- «la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo»;
- «que solo o conjuntamente con otros»;
- «determine los fines y los medios del tratamiento de datos personales».

El primer componente se refiere al aspecto personal de la definición. El tercer componente contiene elementos esenciales para distinguir al responsable de otros agentes y el segundo componente evoca la posibilidad de un «control plural». Estos componentes están estrechamente interrelacionados. No obstante, debido a la metodología que se va a seguir en el presente dictamen, cada uno de estos tres componentes se analizará por separado.

Por razones prácticas, resulta útil empezar por el *primer elemento* del tercer componente, a saber, el significado de la palabra «determine», y continuar después con el resto del tercer componente, antes de abordar por fin los dos primeros componentes.

III.1.a) Elemento preliminar: «determine»

Como se ha señalado anteriormente, el concepto de responsable del tratamiento desempeñaba un papel menor en el Convenio 108. En el artículo 2 del Convenio, la «autoridad controladora del fichero» se definía como organismo «que [es] competente [...] para decidir». El Convenio enfatiza la necesidad de una instancia competente determinada «con arreglo a la ley nacional». Por ello, el Convenio remite a las legislaciones nacionales sobre protección de datos que, según la exposición de motivos, contienen «criterios precisos para determinar quién es la persona competente».

Mientras la primera propuesta de la Comisión refleja esta disposición, la propuesta modificada se refiere, en cambio, al organismo «que decide», eliminando por tanto la necesidad de que la competencia de decidir sea establecida por ley; es decir, la determinación por ley sigue siendo posible, pero ya no es necesaria. Esto se ve confirmado después por la Posición Común del Consejo y el texto adoptado, que se refieren ambos al organismo «que determin[a]».

Dados estos antecedentes, el desarrollo histórico pone de relieve dos elementos importantes: en primer lugar, que es posible ser responsable del tratamiento independientemente de que se haya obtenido por ley la competencia o el mandato específico de controlar datos; en segundo lugar, que en el proceso de adopción de la Directiva 95/46 la determinación del responsable del tratamiento se convierte en un concepto comunitario, un concepto que tiene un significado autónomo en el Derecho comunitario y no está sujeto a variaciones derivadas de posibles divergencias entre las disposiciones de las legislaciones nacionales. Este último elemento es esencial con vistas a garantizar la aplicación efectiva de la Directiva y un alto nivel de protección en los Estados miembros, lo cual requiere una interpretación uniforme y, por tanto, autónoma de un concepto esencial como «responsable del tratamiento», que en la Directiva adquiere una importancia que no tenía en el Convenio 108.

Desde este punto de vista, la Directiva culmina esta evolución al establecer que, aun cuando la capacidad de «determinar» se derive de una atribución específica por ley, tal capacidad procede por lo general de un análisis de los elementos de hecho o de las circunstancias del caso: se debe atender a las operaciones concretas del tratamiento en cuestión y ha de comprenderse quién las determina, respondiendo en un primer momento a las preguntas «por qué se produce este tratamiento?, ¿quién lo ha iniciado?»

Ser responsable del tratamiento es consecuencia, en primer lugar, de la circunstancia de hecho de que un ente ha decidido tratar datos personales para sus propios fines. De hecho, un criterio meramente formal no sería suficiente por al menos dos tipos de razones: en algunos casos, simplemente faltaría el nombramiento formal de un responsable del tratamiento —por ejemplo, por ley, por contrato o mediante notificación de la autoridad de protección de datos—; en otros casos podría ocurrir que el nombramiento formal no reflejara la realidad por haberse encomendado la función de responsable del tratamiento a un organismo que no está de hecho en condiciones de «determinar».

La importancia de la capacidad de influencia de hecho también queda patente en el caso SWIFT¹⁰, en el que esta sociedad se consideró formalmente encargada del tratamiento, pero de hecho actuó —al menos en cierta medida— como responsable del tratamiento. En este caso quedó de manifiesto que, aunque la designación de una parte como responsable o encargado del tratamiento en un contrato puede revelar información pertinente respecto del estatuto jurídico de dicha parte, la designación contractual no es, sin embargo, decisiva a la hora de determinar su estatuto real, que tiene que estar basado en circunstancias concretas.

El enfoque de hecho también se ve respaldado por la consideración de que la Directiva establece que el responsable del tratamiento es quien «determin[a]» más que quien «determina legalmente» los fines y los medios. La determinación efectiva de la responsabilidad es decisiva, aun cuando la designación aparentemente se haya hecho de forma ilegítima o el tratamiento de los datos se realice de manera ilegítima. Es irrelevante si la decisión de procesar datos fue «ilegítima» en el sentido de que el ente que adoptó la decisión tuviera la capacidad legal para hacerlo o el responsable del tratamiento fuera formalmente designado con arreglo a un procedimiento particular. La cuestión de la legalidad del tratamiento de datos personales será pertinente en otra fase y se valorará a la luz de otros artículos (en particular los artículos 6 a 8) de la Directiva. En otras palabras, es importante garantizar que incluso en aquellos casos en que los datos se procesen de forma ilegítima se pueda encontrar fácilmente al responsable del tratamiento y se le pueda atribuir la responsabilidad.

Una última característica del concepto de responsable del tratamiento es su autonomía, en el sentido de que, aunque fuentes legales externas puedan ayudar a identificar quién es el responsable, el dicho concepto debería interpretarse fundamentalmente con arreglo a la legislación sobre protección de datos¹¹. El concepto de responsable del tratamiento no debería verse afectado por otros conceptos —con los que a veces colisiona o se solapa— de otros ámbitos del Derecho, como el de autor o titular de derechos de propiedad intelectual. El ser titular de derechos de propiedad intelectual no excluye la posibilidad de ser también «responsable del tratamiento» y estar, por tanto, sujeto a las obligaciones que se derivan de la legislación sobre protección de datos.

Necesidad de una tipología

El concepto de responsable del tratamiento es un concepto funcional, destinado a asignar responsabilidades en función de la capacidad de influencia de hecho y, por tanto, está basado en un análisis de hecho más que formal. En consecuencia, determinar el control puede requerir en ocasiones una investigación en profundidad y de larga duración. Ahora bien, la necesidad de garantizar la eficacia requiere la adopción de un enfoque pragmático a fin de garantizar la previsibilidad en relación con el control. Desde esta perspectiva, son necesarias unas reglas orientativas y unas presunciones prácticas para orientar y simplificar la aplicación del Derecho de protección de datos.

¹⁰ Este caso se refiere a la transferencia a las autoridades estadounidenses, con fines de lucha contra la financiación del terrorismo, de datos bancarios recogidos por SWIFT para la realización de transacciones financieras por cuenta de bancos y entidades financieras.

¹¹ Véase a continuación la interferencia con conceptos existentes en otras áreas del Derecho (por ejemplo, el concepto de titular de derechos de protección intelectual o de investigaciones científicas, o la responsabilidad conforme al Derecho civil).

Esto exige una interpretación de la Directiva que garantice que el «organismo determinante» pueda identificarse en la mayoría de las situaciones con facilidad y claridad remitiendo a aquellas circunstancias —de hecho o de derecho— de las que habitualmente se puede inferir una capacidad de influencia de hecho, salvo que otros elementos indiquen lo contrario.

Estas circunstancias pueden analizarse y clasificarse con arreglo a las tres categorías de situaciones siguientes, que permiten un enfoque sistematizado de estos asuntos:

1) *Control emanado de una competencia legal explícita*. Entre otros, éste es el caso al que se refiere la segunda parte de la definición, es decir, cuando la designación del responsable del tratamiento o los criterios específicos de su nombramiento se establecen en el Derecho nacional o comunitario. El nombramiento explícito de un responsable del tratamiento por ley no es frecuente y, en general, no plantea grandes problemas. En algunos países, la legislación nacional establece que las autoridades públicas son responsables del procesamiento de datos personales en el marco de sus obligaciones.

No obstante, es más frecuente el caso en que la legislación, más que nombrar directamente al responsable del tratamiento o fijar los criterios de su nombramiento, establece un cometido o impone a alguien la responsabilidad de recoger y tratar determinados datos. Por ejemplo, éste sería el caso de un ente al que se le encargan ciertos cometidos públicos (por ejemplo, la seguridad social) que no se pueden realizar sin recoger al menos algunos datos personales, y que por tanto crea un registro para llevarlos a cabo. En este caso, se deduce de la legislación quién es el responsable del tratamiento. Con mayor frecuencia, la ley puede imponer a entes públicos o privados la obligación de conservar o facilitar determinados datos. Estos entes se considerarían en principio los responsables de cualquier tratamiento de datos personales en ese contexto.

2) *Control emanado de una competencia jurídica implícita*. Se da este caso cuando la capacidad de determinar no se establece explícitamente por ley ni es consecuencia directa de disposiciones legales explícitas, pero sigue emanando de normas jurídicas comunes o de la práctica jurídica en distintos ámbitos (Derecho civil, mercantil, laboral, etc.). En este caso, las funciones tradicionales existentes que suelen implicar una cierta responsabilidad ayudarán a identificar al responsable del tratamiento: por ejemplo, el empleador en relación con los datos sobre sus empleados, el editor respecto de los datos de sus suscriptores o la asociación respecto de los datos de sus socios o contribuyentes.

En todos estos casos, la capacidad para determinar las actividades de tratamiento puede considerarse vinculada por su naturaleza a la función de una organización (privada), que en última instancia también conlleva responsabilidades desde el punto de vista de la protección de datos. En términos legales esto se aplicaría independientemente de que la capacidad de determinar se confiriera a los organismos jurídicos mencionados o fuera ejercida por los órganos competentes por su cuenta o por una persona física en una función similar (véase a continuación el primer elemento de la letra c). Ahora bien, esto mismo se aplicaría a una autoridad pública con determinados cometidos administrativos en un país en el que la legislación no fuera explícita en lo relativo a su responsabilidad sobre la protección de datos.

Ejemplo nº 1: Operadores de telecomunicaciones

El papel de los operadores de telecomunicaciones es un ejemplo interesante de orientación jurídica para el sector privado: el considerando 47 de la Directiva 95/46/CE aclara que «*cuando un mensaje con datos personales sea transmitido a través de un servicio de telecomunicaciones o de correo electrónico cuyo único objetivo sea transmitir mensajes de ese tipo, será considerada normalmente responsable del tratamiento de los datos personales presentes en el mensaje aquella persona de quien proceda el mensaje y no la que ofrezca el servicio de transmisión; [...] no obstante, las personas que ofrezcan estos servicios normalmente serán consideradas responsables del tratamiento de los datos personales complementarios y necesarios para el funcionamiento del servicio*». Por lo tanto, los proveedores de servicios de telecomunicaciones en principio sólo deberían considerarse responsables del tratamiento de los datos sobre el tráfico y la facturación, pero no de los datos transmitidos¹². Esta orientación jurídica del legislador comunitario concuerda plenamente con el enfoque funcional adoptado en el presente dictamen.

3) Control emanado de una capacidad de influencia de hecho. Éste es el caso cuando la responsabilidad del tratamiento se asigna sobre la base de una evaluación de las circunstancias de hecho. En muchos casos, esto conllevará una evaluación de las relaciones contractuales entre las distintas partes implicadas. Esta evaluación permite sacar conclusiones externas que atribuyan la función y responsabilidades de responsable del tratamiento a una o varias partes. Esto puede resultar particularmente útil en entornos complejos que suelen recurrir a las nuevas tecnologías de la información y en los que los agentes pertinentes tienden a verse a sí mismos como «mediadores» y no como responsables del tratamiento.

Puede ocurrir que un contrato no diga nada sobre quién es el responsable del tratamiento y, sin embargo, contenga elementos suficientes para asignar la función de responsable del tratamiento a una parte que manifiestamente ejerce un papel dominante en este sentido. También es posible que el contrato sea más explícito en cuanto al responsable del tratamiento. Si no hay motivos para dudar que esto refleja debidamente la realidad, nada se opone a que se sigan las condiciones fijadas en el contrato. No obstante, las condiciones de un contrato no son determinantes en todas las circunstancias, puesto que esto permitiría a las partes asignar la responsabilidad simplemente donde lo consideren oportuno.

El propio hecho de que alguien determine cómo se procesan los datos personales puede implicar su condición de responsable del tratamiento de datos, aun cuando tal condición surja fuera del ámbito de una relación contractual o sea explícitamente excluida por un contrato. Un ejemplo claro de esto fue el caso SWIFT, en el que esta empresa tomó la decisión de poner a disposición determinados datos personales —que inicialmente se habían tratado con fines comerciales por cuenta de unas entidades financieras— para su

¹² Una autoridad de protección de datos trató la cuestión de la responsabilidad del tratamiento en un asunto en que un interesado denunció la publicidad por correo electrónico no solicitada. En la denuncia, el interesado pidió al proveedor de la red de comunicación que o bien confirmara o denegara que era el remitente del correo electrónico de publicidad. La autoridad de protección de datos concluyó que la empresa que sólo facilita a un cliente el acceso a una red de comunicación, es decir, que no inicia la transmisión de datos ni selecciona a los destinatarios ni modifica la información contenida en la transmisión, no puede considerarse que actúe como responsable del tratamiento.

utilización en la lucha contra la financiación del terrorismo, como había solicitado del Departamento del Tesoro de los EE.UU. en diversos requerimientos.

En caso de duda pueden ser de utilidad otros elementos que no sean las condiciones de un contrato para determinar quién es el responsable del tratamiento, como el grado de control real ejercido por una parte, la imagen dada a los interesados o las expectativas razonables de los interesados sobre la base de esta visibilidad (véase a continuación el tercer elemento de la letra b). Esta categoría es particularmente importante puesto que permite examinar las responsabilidades y asignarlas también en aquellos casos de conducta ilegítima en que las actividades efectivas de tratamiento puedan realizarse en contra de los intereses y la voluntad de algunas de las partes.

Conclusión preliminar

Entre estas categorías, las dos primeras permiten, en principio, identificar con mayor seguridad al organismo determinante y posiblemente abarquen más del 80% de las situaciones pertinentes en la práctica. Ahora bien, una designación legal formal debería estar en consonancia con las normas de protección de datos y, por tanto, garantizar que el organismo designado tenga el control efectivo sobre las operaciones de tratamiento o, en otras palabras, que el nombramiento legal refleje la realidad de los hechos.

La categoría 3 requiere un análisis más complejo y es probable que dé lugar a interpretaciones divergentes. Las condiciones de un contrato a menudo pueden ayudar a aclarar la cuestión, pero no son determinantes en todas las circunstancias. Hay un número creciente de agentes que no consideran que sean ellos quienes determinan las actividades de tratamiento y, por tanto, no se sienten responsables de éstas. En tales casos, la única opción viable es una conclusión sobre la base de la capacidad de influencia de hecho. La cuestión de la legitimidad de este tratamiento se evaluará a la luz de otros artículos (6 a 8).

Si no cabe aplicar ninguna de las categorías mencionadas, el nombramiento de un responsable del tratamiento debería considerarse nulo de pleno derecho. En efecto, un organismo que no tenga capacidad de influencia de hecho ni de derecho para determinar cómo se tratan los datos personales no puede considerarse responsable del tratamiento.

Desde un punto de vista formal, este enfoque se ve corroborado por el hecho de que la definición del responsable del tratamiento debe considerarse una disposición jurídica vinculante de la que las partes no pueden desviarse o sustraerse sin más. Desde un punto de vista estratégico, tal nombramiento sería contrario a la aplicación efectiva de la legislación sobre la protección de datos e invalidaría la responsabilidad que implica el tratamiento de datos.

III.1.b) Tercer elemento: «fines y medios del tratamiento»

El tercer elemento representa la parte sustantiva de la prueba: lo que una parte debe determinar para que se la pueda considerar responsable del tratamiento.

La historia de esta disposición presenta varios aspectos. El Convenio 108 se refería al fin de los ficheros automatizados, a las categorías de datos personales y a las operaciones que se les podían aplicar. La Comisión asumió estos elementos sustantivos, con modificaciones lingüísticas menores, y les sumó la competencia de decidir qué terceros podían tener acceso a los datos. La propuesta modificada de la Comisión dio un paso adelante al sustituir «los fines del fichero» por «los fines y el objetivo del tratamiento», pasando por tanto de una definición estática vinculada a un fichero a una definición

dinámica vinculada a la actividad del tratamiento. La propuesta modificada seguía refiriéndose a los cuatro elementos (fines/objetivo, datos personales, operaciones y terceras partes que tienen acceso a los datos), que sólo se redujeron a dos («fines y medios») en la Posición Común del Consejo.

Los diccionarios definen la palabra «fin» como un « resultado anticipado que se persigue o que guía la actuación prevista» y la palabra «medio» como «la manera en que se obtiene un resultado o se alcanza un objetivo».

Por otra parte, la Directiva establece que los datos deben recogerse con fines determinados, explícitos y legítimos y no deben tratarse posteriormente de manera incompatible con dichos fines. La determinación de los «fines» del tratamiento y de los «medios» para alcanzarlos reviste, por tanto, una importancia particular.

También puede afirmarse que la determinación de los fines y los medios equivale a determinar, respectivamente, el «por qué» y el «cómo» de ciertas actividades de tratamiento. Desde esta perspectiva, y teniendo en cuenta que ambos elementos van unidos, es necesario ofrecer orientación sobre el nivel de influencia en lo relativo al «por qué» y al «cómo» que puede conllevar la consideración de un ente como responsable del tratamiento.

A la hora de evaluar la determinación de los fines y los medios con vistas a asignar la función de responsable del tratamiento, la pregunta crucial que se plantea por tanto es hasta qué nivel de detalle debe determinar una persona los fines y medios para que se la considere responsable del tratamiento. Y de forma correlativa a ello, cuál es el margen de maniobra que la Directiva le otorga al encargado del tratamiento de datos. Estas definiciones adquieren una pertinencia particular cuando son varios los agentes implicados en el tratamiento de datos personales y resulta necesario determinar quién es responsable del tratamiento (solo o conjuntamente con otros) y quién debe considerarse, en cambio y llegado el caso, encargado del tratamiento.

El énfasis que ha de ponerse en los fines o en los medios puede variar dependiendo del contexto específico en el que tiene lugar el tratamiento.

Es necesario un enfoque pragmático que ponga mayor énfasis en la discrecionalidad para determinar los fines y la flexibilidad para adoptar decisiones. En estos casos, la pregunta es por qué se produce el tratamiento y cuál es el papel de los agentes posiblemente implicados, como las empresas externalizadoras: ¿habría procedido al tratamiento de datos la empresa externalizada si no se lo hubiera pedido el responsable del tratamiento, y en qué condiciones? Un encargado del tratamiento podría seguir las instrucciones generales recibidas en lo relativo especialmente a los fines y no profundizar demasiado en los medios.

Ejemplo nº 2: Publicidad por correo electrónico

La empresa ABC suscribe contratos con distintas organizaciones para realizar campañas de publicidad por correo electrónico y ocuparse de los pagos. Da instrucciones precisas a tal fin (qué material de publicidad ha de enviarse, a quién, cómo debe pagarse, qué cantidades, en qué fechas, etc.). A pesar de que las organizaciones tienen algún margen discrecional (incluido en lo referente al *software* que van a utilizar), sus cometidos están definidos con bastante claridad y precisión y, aunque la empresa responsable de la distribución del correo pueda brindar asesoramiento (por ejemplo, desaconsejando el envío de correo en agosto), están claramente sujetas a actuar según las instrucciones de ABC. Además, sólo un ente, la empresa ABC, tiene el derecho de usar los datos procesados; los demás entes tendrían que remitir a la base legal de la empresa ABC en caso de que se cuestionara su capacidad jurídica para tratar los datos. En este caso está claro que la empresa ABC es la responsable del tratamiento de los datos y cada una de las demás organizaciones puede considerarse encargada del tratamiento en lo relativo al tratamiento específico de datos realizado por cuenta de aquélla.

Por lo que se refiere a la determinación de los medios, el término «medios» abarca evidentemente distintos tipos de elementos, como lo ilustra la historia de esta definición. En la propuesta original, el papel del responsable del tratamiento emanaba de la determinación de cuatro elementos (fines/objetivo, datos personales, operaciones y terceros que tienen acceso a los datos). No cabe interpretar que la formulación final de la disposición, que sólo hace referencia a «los fines y los medios», esté en contradicción con la versión antigua, dado que no puede haber duda alguna sobre el hecho de que, por ejemplo, el responsable del tratamiento debe determinar qué datos deben procesarse para los fines previstos. Por lo tanto, la definición final debe entenderse más bien como una versión abreviada que recoge, sin embargo, el sentido de la versión antigua. En otras palabras, los «medios» no sólo se refieren a los medios técnicos de tratar los datos personales, sino también al «cómo» del tratamiento, que incluye preguntas como «¿qué datos deben tratarse?», «¿qué terceros deben tener acceso a estos datos?», «¿cuándo deben borrarse los datos?», etc.

Por lo tanto, la determinación de los «medios» abarca preguntas técnicas y organizativas cuando la decisión puede delegarse en los encargados del tratamiento (como, por ejemplo, «¿qué *hardware* o *software* debe usarse?») y elementos esenciales que tradicionalmente y de forma inherente se reservaban para la determinación del responsable del tratamiento, como «¿qué datos deben tratarse?», «durante cuánto tiempo deben tratarse?», «¿quién debe tener acceso a ellos?», etc.

En estas circunstancias, mientras la determinación de los fines del tratamiento desembocaría en cualquier caso en la determinación del responsable del tratamiento, la determinación de los medios sólo implicaría un control si afectara a elementos esenciales de los medios.

Desde esta perspectiva, es perfectamente posible que los medios técnicos y organizativos los determine exclusivamente el encargado del tratamiento de los datos.

En estos casos —es decir, cuando hay una buena definición de los fines, pero poca o ninguna orientación sobre los medios técnicos y organizativos— los medios deberían representar una vía razonable para alcanzar el o los fines y el responsable del tratamiento debería estar plenamente informado de los medios utilizados. Si una parte en un contrato tuviera una influencia sobre el fin y llevara a cabo el tratamiento (también) en su propio beneficio, por ejemplo utilizando datos personales recibidos con vistas a generar servicios de valor añadido, sería el responsable del tratamiento (o posiblemente un

encargado del tratamiento junto con otros) para otra actividad de tratamiento y, por tanto, estaría sujeto a todas las obligaciones de la legislación de protección de datos aplicable.

Ejemplo nº 3: Empresa considerada encargada del tratamiento, pero que actúa como responsable del tratamiento

La empresa MarketinZ presta servicios de publicidad promocional y *marketing* directo a varias empresas. La empresa GoodProductZ firma un contrato con MarketinZ con arreglo al cual esta última realiza publicidad comercial para los clientes de la primera y es considerada encargada del tratamiento de datos. Ahora bien, MarketinZ decide utilizar la base de datos de clientes de GoodProducts también para promocionar los productos de otros clientes. Esta decisión de añadir un fin adicional al fin con el que se transfirieron los datos personales convierte a MarketinZ en responsable del tratamiento de datos respecto de esta operación de tratamiento. La cuestión de la legitimidad de este tratamiento se evaluará a la luz de otros artículos (6 a 8).

En algunos sistemas jurídicos las decisiones adoptadas sobre medidas de seguridad son particularmente importantes puesto que tales medidas se consideran explícitamente una característica esencial que ha de definir el responsable del tratamiento. Esto plantea la cuestión de qué decisiones en materia de seguridad determinan la condición de responsable del tratamiento en el caso de una empresa a la que se haya externalizado el tratamiento.

Conclusión preliminar

La determinación del «fin» del tratamiento es competencia del «responsable del tratamiento». Por consiguiente, quienquiera que tome esta decisión es (*de facto*) el responsable del tratamiento. Éste puede delegar la determinación de los «medios» del procesamiento en la medida en que se trate de cuestiones técnicas u organizativas. Las cuestiones de fondo que sean esenciales a efectos de la legitimidad del tratamiento son competencia del responsable del tratamiento. Una persona o un ente que decida, por ejemplo, cuánto tiempo se almacenarán los datos o que tenga acceso a los datos tratados actúa como responsable del tratamiento respecto de esta parte del uso de los datos y, por tanto, debe cumplir todas las obligaciones que incumben a un responsable del tratamiento.

III.1.c) Primer elemento: «persona física o jurídica o cualquier otro organismo»

El primer elemento de la definición se refiere a la vertiente personal: quién puede ser responsable del tratamiento y, por tanto, considerado en última instancia responsable de las obligaciones que emanan de la Directiva. La definición refleja exactamente la formulación del artículo 2 del Convenio 108 y no fue objeto de debate específico en el proceso decisorio de la Directiva. Se refiere a una amplia gama de sujetos que pueden desempeñar la función de responsable del tratamiento y que va de las personas físicas a las jurídicas, pasando por «cualquier otro organismo».

Es importante que la interpretación de este elemento garantice la aplicación efectiva de la Directiva al favorecer en lo posible una identificación clara y unívoca del responsable del tratamiento en todas las circunstancias, independientemente de que se haya producido y hecho público un nombramiento formal.

En primer lugar es importante ajustarse en lo posible a la práctica establecida tanto en el sector público como en el privado en otras áreas del Derecho, como el civil, el administrativo o el penal. En la mayoría de los casos, estas disposiciones indicarán a qué personas u organismos deben asignarse las responsabilidades y, en principio, ayudarán a determinar quién es el responsable del tratamiento de datos.

Desde la óptica estratégica de la asignación de responsabilidades y a fin de proporcionar a los interesados un ente de referencia más estable y fiable para el ejercicio de sus derechos en virtud de la Directiva, preferentemente debe considerarse responsable del tratamiento a la empresa o al organismo como tal antes que a una persona concreta dentro de la empresa o el organismo. En última instancia, debe considerarse responsable del tratamiento de datos y de las obligaciones que emanan de la legislación de protección de datos a la empresa o al organismo, a no ser que haya elementos inequívocos que indiquen que el responsable debe ser una persona física. En general, debe presumirse que una empresa o un organismo público es responsable como tal de las actividades de tratamiento que tengan lugar dentro su ámbito de actividades y riesgos.

En ocasiones, las empresas y los organismos públicos nombran a una persona concreta como responsable de la ejecución de las operaciones de tratamiento. No obstante, también en el caso de que una persona física concreta sea nombrada para velar por el cumplimiento de los principios de protección de datos o para tratar datos personales, ésta no será la responsable del tratamiento, sino que actuará por cuenta del ente jurídico (empresa u organismo público), que es el que tendrá que responder en su calidad de responsable del tratamiento en caso de incumplimiento de los principios¹³.

Una cuestión crucial de «gobernanza de la protección de datos», especialmente en estructuras grandes y complejas, es garantizar tanto una clara responsabilidad de la persona física que representa a la empresa como unas responsabilidades funcionales concretas dentro de la estructura, por ejemplo encargando a otras personas que actúen como representantes o puntos de contacto de los interesados.

Es necesario un análisis especial en los casos en que una persona física que actúe por cuenta de una persona jurídica utilice datos para sus propios fines, fuera del ámbito y del posible control de las actividades de la persona jurídica. En este caso, la persona física en cuestión sería la responsable del tratamiento que hubiera decidido realizar y asumiría la responsabilidad sobre dicha utilización de los datos personales. No obstante, el responsable del tratamiento original conservaría alguna responsabilidad en caso de que ese tratamiento adicional se produjera debido a la falta de medidas de seguridad adecuadas.

Como ya se ha mencionado anteriormente, la función de responsable del tratamiento es fundamental y particularmente importante a la hora de determinar la responsabilidad y de imponer sanciones. A pesar de que la responsabilidad y las sanciones varíen de unos Estados miembros a otros, puesto que tales sanciones se imponen con arreglo al Derecho nacional, la necesidad de determinar claramente a la persona física o jurídica responsable de las infracciones de la legislación de protección de datos es sin lugar a dudas una condición previa esencial para la aplicación efectiva de la Directiva.

¹³ Un razonamiento similar se aplica en relación con el Reglamento (CE) 45/2001, cuyo artículo 2, letra d), se refiere a «la institución, organismo, dirección general, unidad u otra entidad organizativa comunitaria». Ha quedado sentado en la práctica de la supervisión que los funcionarios de las instituciones y organismos de la UE que han sido nombrados «responsable del tratamiento», actúan en nombre del organismo para el que trabajan.

La determinación del «responsable del tratamiento» desde la perspectiva de la protección de datos estará interrelacionada en la práctica con las normas civiles, administrativas o penales que establecen la atribución de responsabilidades o sanciones a que pueden quedar sujetas las personas físicas o jurídicas¹⁴.

La responsabilidad civil no debería plantear problemas particulares en este contexto dado que se aplica, en principio, tanto a las personas jurídicas como a las personas físicas. En cambio, la responsabilidad penal y/o administrativa podría en ciertas ocasiones, dependiendo de la legislación nacional, ser aplicable solamente a las personas físicas. Si las respectivas legislaciones nacionales contemplan sanciones penales o administrativas para las infracciones de la protección de datos, tales legislaciones determinarán en principio también quién es el responsable: si no se reconoce la responsabilidad penal o administrativa de las personas jurídicas, tal responsabilidad será asumida por funcionarios o personas jurídicas con arreglo a las normas particulares de la legislación nacional¹⁵.

El Derecho europeo contiene ejemplos ilustrativos de criterios que atribuyen la responsabilidad penal¹⁶, en particular cuando se produce un delito en beneficio de la persona jurídica: en tales casos, la responsabilidad se puede atribuir a «cualquier persona, a título individual o como parte de un órgano de la persona jurídica [...] basada en:

- a) un poder de representación de la persona jurídica;
- b) una autoridad para tomar decisiones en nombre de la persona jurídica; o
- c) una autoridad para ejercer control dentro de la persona jurídica».

Conclusión preliminar

Resumiendo las reflexiones expuestas cabe concluir que quien debe responder de la infracción de la protección de datos es siempre el responsable del tratamiento, es decir, la persona jurídica (empresa u organismo público) o la persona física que formalmente se haya determinado como tal con arreglo a los criterios de la Directiva. Si una persona física que trabaja en una empresa u organismo público utiliza los datos para sus propios fines, al margen de las actividades de la empresa, dicha persona se considerará *de facto* el responsable del tratamiento y tendrá que responder como tal.

¹⁴ Véase el «Estudio comparativo sobre la situación en los 27 Estados miembros en lo relativo a la legislación aplicable a las obligaciones no contractuales derivadas de infracciones del derecho a la intimidad y de derechos de la personalidad» de la Comisión, de febrero de 2009, disponible en: http://ec.europa.eu/justice_home/doc_centre/civil/studies/doc/study_privacy_en.pdf

¹⁵ Esto no excluye que las leyes nacionales puedan contemplar la responsabilidad penal o administrativa no sólo del responsable del tratamiento, sino también de cualquier persona que infrinja la normativa de protección de datos.

¹⁶ Véase, por ejemplo, la Directiva 2008/99/CE, de 19 de noviembre de 2008, relativa a la protección del medio ambiente mediante el Derecho penal, o la Decisión Marco del Consejo, de 13 de junio de 2002, sobre la lucha contra el terrorismo. Los instrumentos legales se basan bien en los artículos 29, 31.e) y 34.2.b) del TUE o bien se ajustan a las bases jurídicas de los instrumentos utilizados en el primer pilar, que se derivan de la jurisprudencia del TJCE en los asuntos C-176/03, Comisión/Consejo, [Rec.] 2005, I-7879 y C-440/05, Comisión/Consejo, [Rec.] 2007, I-9097. Véase también la Comunicación COM (2005) 583 final.

Ejemplo nº 4: Vigilancia secreta de empleados

Un miembro de la dirección de una empresa decide vigilar en secreto a los empleados de la empresa a pesar de que esta decisión no ha sido formalmente respaldada por la dirección. La empresa debe considerarse responsable del tratamiento y hacer frente a las posibles denuncias y responsabilidades ante los empleados de cuyos datos personales se haya hecho un uso abusivo.

La responsabilidad de la empresa se debe, en particular, al hecho de que, en su calidad de responsable del tratamiento, tiene la obligación de velar por el cumplimiento de las normas de seguridad y confidencialidad. El uso abusivo por parte de un directivo o empleado de la empresa podría considerarse como el resultado de unas medidas de seguridad inadecuadas. Esto es independiente de que, en una fase posterior, también puedan considerarse responsables el citado miembro de la dirección u otras personas físicas de la empresa, tanto desde el punto de vista civil —también frente a la empresa— como penal. Este sería el caso, por ejemplo, si el miembro de la dirección utilizara los datos recogidos para extorsionar a los empleados y obtener favores personales: se le consideraría entonces «responsable del tratamiento» y tendría que responder de ese uso particular de los datos.

III.1.d) Segundo elemento: «solo o conjuntamente con otros»

Este párrafo, basado en el análisis previo de las características típicas de un responsable del tratamiento, abordará aquellos casos en que varios agentes interactúan en el tratamiento de datos personales. De hecho, hay un número creciente de casos en que diferentes agentes actúan como responsable del tratamiento y la definición establecida en la Directiva contempla este supuesto.

La posibilidad de que el responsable del tratamiento actúe «solo o conjuntamente con otros» no se mencionaba en el Convenio 108 y, de hecho, la introdujo el Parlamento Europeo antes de la adopción de la Directiva. En el dictamen de la Comisión sobre la enmienda del PE, la Comisión menciona la posibilidad de que *«varias partes determinen conjuntamente, para una única operación de tratamiento, los fines y los medios del tratamiento que se vaya a llevar a cabo»* y, por lo tanto, en tal caso, *«cada uno de estos corresponsables del tratamiento debe considerarse vinculado por las obligaciones impuestas por la Directiva de proteger a las personas físicas cuyos datos se estén tratando»*.

El dictamen de la Comisión no reflejaba completamente las complejidades de la situación real del tratamiento de datos en la actualidad, puesto que se centraba sólo en un supuesto en el que todos los responsables del tratamiento determinan por igual y son igualmente responsables de una única operación de tratamiento. La realidad, en cambio, demuestra que ésta sólo es una de las distintas formas de «control plural» que pueden darse. Desde esta óptica, debe interpretarse que «conjuntamente» significa «junto con otros» o «no solo» y puede revestir distintas formas y combinaciones.

En primer lugar, debe señalarse que la probabilidad de que haya varios agentes implicados en el tratamiento de datos personales está vinculada de forma natural a distintos tipos de actividades que, con arreglo a la Directiva, pueden equivaler al «tratamiento», que a fin de cuentas es el objeto del «control conjunto». La definición de tratamiento contenida en el artículo 2.b) de la Directiva no excluye la posibilidad de que distintos agentes estén implicados en diferentes operaciones o conjuntos de operaciones

en materia de datos personales. Estas operaciones pueden producirse simultáneamente o en distintas fases.

En un entorno de tal complejidad es aún más importante que las funciones y responsabilidades puedan asignarse con facilidad, de modo que se garantice que las complejidades del control conjunto no den lugar a un reparto inviable de responsabilidades que minaría la eficacia de la normativa sobre protección de datos. Desgraciadamente, debido a la variedad de soluciones posibles no puede establecerse una lista o categorización exhaustiva y «cerrada» de los distintos tipos de «control conjunto». No obstante, en este contexto también resulta útil brindar orientación tanto a través de categorías y ejemplos de control conjunto como por medio de elementos de hecho de los que quepa inferir o presumir un control conjunto.

En general, la evaluación del control conjunto debería ser un reflejo de la evaluación del control «único» expuesta en las letras a) a c) del apartado III.1. En la misma línea, evaluar el control conjunto también debería adoptarse un enfoque sustantivo y funcional, como se ha ilustrado anteriormente, centrado en establecer si los fines y los medios los determina más de una parte.

Ejemplo nº 5: Instalación de cámaras de videovigilancia

El propietario de un inmueble firma un contrato con una empresa de seguridad por el que esta última instala por cuenta del responsable del tratamiento unas cámaras en distintos puntos del inmueble. Los fines de la videovigilancia y la manera en que se recogen y almacenan las imágenes los determina exclusivamente el propietario del inmueble, por lo que éste debe considerarse el único responsable del tratamiento a efectos de esta operación.

En este contexto también pueden ser útiles para evaluar el control conjunto los acuerdos contractuales, pero éstos siempre deben valorarse a la luz de las circunstancias de hecho de la relación entre las partes.

Ejemplo nº 6: Cazatalentos

La empresa Headhunterz Ltd ayuda a la empresa Enterprize Inc a contratar personal nuevo. El contrato establece claramente que «Headhunterz Ltd actuará en nombre de Enterprize y al tratar datos personales actuará como encargado del tratamiento de datos. Enterprize es el único responsable del tratamiento de datos». No obstante, Headhunterz Ltd se encuentra en una posición ambigua: por un lado, desempeña el papel de responsable del tratamiento frente a las personas que buscan un empleo y, por otro, asume el papel de encargado del tratamiento que actúa en nombre del responsable del tratamiento, como Enterprize Inc y otras empresas que buscan personal con su ayuda. Además, Headhunterz —que es famosa por su servicio de valor añadido «global matchz»— busca a los candidatos idóneos tanto entre los CV recibidos directamente por Enterprize como entre los que ya tiene en su gran base de datos propia. Esto hace que Headhunterz, que con arreglo al contrato sólo recibe remuneración por los contratos efectivamente firmados, mejore la correspondencia entre ofertas de trabajo y personas en busca de empleo, aumentando así sus ingresos. Habida cuenta de los elementos expuestos cabe afirmar que, a pesar de lo establecido en el contrato, Headhunterz Ltd debe considerarse responsable del tratamiento y, además, que controla conjuntamente con Enterprize Inc cuando menos el conjunto de operaciones relacionadas con las contrataciones de Enterprize.

Desde este punto de vista, existe control conjunto cuando las diferentes partes determinan, respecto de unas operaciones de tratamiento específicas, o bien los fines o bien aquellos elementos esenciales de los medios que caracterizan al responsable del tratamiento (véanse las letra a) a c) del apartado III.1).

No obstante, en el contexto del control conjunto, la participación de las partes en la determinación conjunta puede revestir distintas formas y el reparto no tiene que ser necesariamente a partes iguales. De hecho, cuando son varios los agentes, estos pueden tener una relación muy estrecha entre sí (y compartir, por ejemplo, todos los fines y medios de un tratamiento), o bien una relación más laxa (y, por ejemplo, compartir sólo los fines o los medios, o una parte de éstos). Por lo tanto, debe tomarse en consideración una amplia variedad de tipologías de control conjunto y analizarse sus consecuencias legales, procediendo con cierta flexibilidad para tener en cuenta la creciente complejidad de la realidad actual del tratamiento de datos.

Habida cuenta de estas circunstancias, es necesario examinar los diferentes grados de interacción o relación que pueda haber entre las múltiples partes implicadas en el tratamiento de datos personales.

En primer lugar, el mero hecho de que diferentes partes cooperen en el tratamiento de datos personales, por ejemplo en cadena, no implica que sean conjuntamente responsables del tratamiento en todos los casos, puesto que un intercambio de datos entre dos partes que no compartan fines y medios para un conjunto de operaciones comunes podría considerarse solamente como una transferencia de datos entre responsables del tratamiento que actúan por separado.

Ejemplo nº 7: Agencia de viajes (1)

Una agencia de viajes envía datos personales de sus clientes a una compañía aérea y a una cadena hotelera para hacer las reservas de un paquete de viaje. La compañía aérea y el hotel confirman la disponibilidad de los asientos y habitaciones solicitados. La agencia de viajes emite los documentos de viaje y talones para sus clientes. En este caso, la agencia de viajes, la compañía aérea y el hotel serán tres responsables del tratamiento distintos, cada uno de los cuales estará sujeto a las obligaciones en materia de protección de datos que correspondan a su propio tratamiento de datos personales.

Sin embargo, la evaluación puede ser distinta en el supuesto de que varios agentes decidan crear una infraestructura compartida para perseguir sus propios fines. Cuando dichos agentes determinen, a la hora de crear esa infraestructura, los elementos esenciales de los medios que vayan a usar, se convierten conjuntamente en responsables del tratamiento de datos —al menos a ese respecto—, aun cuando no compartan necesariamente los mismos fines.

Ejemplo nº 8: Agencia de viajes (2)

La agencia de viajes, la cadena hotelera y la compañía aérea deciden crear una plataforma común en internet para mejorar su cooperación en el ámbito de la gestión de las reservas de viajes. Acuerdan los elementos importantes de los medios que van a utilizar, como el tipo de datos que se almacenarán, la forma en que se realizarán y confirmarán las reservas o quién tendrá acceso a la información almacenada. Además, deciden compartir los datos de sus clientes para realizar acciones integradas de *marketing*.

En este caso, la agencia de viajes, la aerolínea y la cadena hotelera tendrán un control conjunto sobre la manera en que se tratarán los datos personales de sus clientes respectivos y, por lo tanto, serán conjuntamente responsables del tratamiento en lo relativo a las operaciones de tratamiento relacionadas con su plataforma común de reservas en internet. Sin embargo, cada uno de ellos seguiría manteniendo el control exclusivo respecto de otras actividades de tratamiento, por ejemplo las relacionadas con la gestión de sus recursos humanos.

En algunos casos, varios agentes tratan los mismos datos personales de forma consecutiva. En tales supuestos, es probable que, a micronivel, las distintas operaciones de tratamiento de la cadena parezcan desconectadas entre sí, puesto que cada una de ellas puede tener un fin diferente. Sin embargo, es necesario hacer un doble control para determinar si, a macronivel, estas operaciones de tratamiento no deberían considerarse un «conjunto de operaciones» que persiguen un fin común o utilizan unos medios establecidos conjuntamente.

Los siguientes dos ejemplos aclaran esta idea al presentar dos posibles escenarios distintos.

Ejemplo nº 9: Transferencia de datos sobre empleados a las autoridades de Hacienda

La empresa XYZ recoge y procesa datos personales de sus empleados con el fin de gestionar salarios, misiones, seguros de enfermedad, etc. Pero la legislación también impone a la empresa la obligación de enviar todos los datos sobre los salarios a las autoridades de Hacienda, con vistas a reforzar el control fiscal.

En este caso, aunque tanto la empresa XYZ como las autoridades fiscales traten los mismos datos relativos a los salarios, la falta de unos fines o medios compartidos respecto de tal tratamiento de datos dará lugar a que ambos entes se consideren responsables del tratamiento de datos independientes.

Ejemplo nº 10: Transacciones financieras

Tomemos, por el contrario, el caso de un banco que utiliza un servicio de mensajería financiera para realizar sus transacciones financieras. El banco y la empresa de mensajería se ponen de acuerdo en cuanto a los medios para el tratamiento de los datos financieros. El tratamiento de datos personales relativos a transacciones financieras lo realiza en una primera fase la entidad financiera y, sólo en una fase ulterior, la empresa de mensajería financiera. Ahora bien, aun cuando, a micronivel, cada uno de estos agentes persiga su propio fin, a macronivel las distintas fases y fines y medios del tratamiento están estrechamente vinculados. En este caso, puede considerarse que tanto el banco como la empresa de mensajería son responsables del tratamiento de datos conjuntos.

Hay otros supuestos en que los distintos agentes implicados determinan conjuntamente, en algunos casos y en distintos grados, los fines y/o medios de una operación de tratamiento.

Y hay casos en que cada responsable del tratamiento responde sólo de una parte del tratamiento, pero la información se reúne y trata a través de una plataforma.

Ejemplo nº 11: Portales de administración electrónica

Los portales de administración electrónica actúan como intermediarios entre los ciudadanos y las unidades de administración pública: el portal transfiere solicitudes de los ciudadanos y almacena los documentos de la unidad de administración pública hasta que éstos sean reclamados por los ciudadanos. Cada unidad de administración pública sigue siendo responsable del tratamiento de los datos tratados para sus propios fines. No obstante, el portal en sí también puede considerarse responsable del tratamiento. De hecho, trata (es decir, recoge y transfiere a la unidad competente) las solicitudes de los ciudadanos, así como los documentos públicos (es decir, los almacena y regula el acceso a ellos, como la descarga por los ciudadanos) para otros fines (prestación de servicios de administración electrónica) distintos de aquéllos por los que los datos fueron tratados inicialmente por cada una de las unidades de administración pública. Estos responsables del tratamiento, entre otras obligaciones que les incumben, deberán garantizar que el sistema de transferencia de datos personales del usuario al sistema de la administración pública sea seguro, puesto que, a macronivel, esta transferencia es una parte esencial del conjunto de operaciones de tratamiento realizadas a través del portal.

Otra estructura posible es el «enfoque basado en el origen», que se plantea cuando cada uno de los responsables del tratamiento debe responder de los datos que introduce en el sistema. Este es el caso de algunas bases de datos de ámbito europeo, en las que el control —y por tanto la obligación de atender las solicitudes de acceso y rectificación— se asigna sobre la base del origen nacional de los datos personales.

Otro escenario interesante lo proporcionan las redes sociales en línea.

Ejemplo nº 12: Redes sociales

Los proveedores de servicios de redes sociales ponen a disposición plataformas de comunicación en línea que permiten a los usuarios publicar e intercambiar información con otros usuarios. Estos proveedores de servicios son responsables del tratamiento de datos, puesto que determinan tanto los fines como los medios del tratamiento de tal información. Los usuarios de estas redes, que cargan datos personales incluso de terceros, podrían considerarse responsables del tratamiento si sus actividades no quedarán amparadas por la llamada «excepción doméstica»¹⁷.

Una vez analizados los casos en que distintos agentes determinan conjuntamente sólo una parte de los fines y medios, cabe detenerse en el caso muy claro y sencillo en que varios agentes determinan conjuntamente y comparten todos los fines y medios de las actividades de tratamiento, dando lugar a un control conjunto genuino.

En este último caso, es fácil determinar quién es competente y está en condiciones de garantizar los derechos de los interesados y de cumplir las obligaciones en materia de protección de datos. No obstante, la tarea de determinar cuál de los responsables del tratamiento es competente —y debe responder— en relación con los derechos y obligaciones de los interesados es mucho más compleja cuando varios responsables del tratamiento que actúan conjuntamente comparten los fines y medios del tratamiento de forma asimétrica.

Necesidad de aclarar el reparto del control

En primer lugar, hay que destacar, especialmente en casos de control conjunto, que el hecho de no estar en condiciones de cumplir directamente todas las obligaciones que incumben al responsable del tratamiento (facilitar información, derecho de acceso, etc.) no excluye que se sea responsable del tratamiento. Es posible que, en la práctica, tales obligaciones las puedan cumplir fácilmente otras partes —que a veces están más cercanas al interesado— por cuenta del responsable del tratamiento. No obstante, el responsable del tratamiento seguirá siendo, en cualquier caso, el responsable último de las obligaciones y deberá responder de cualquier infracción de éstas.

Con arreglo a un texto previo presentado por la Comisión durante el proceso de adopción de la Directiva, el hecho de tener acceso a determinados datos personales implicaría ser responsable (conjuntamente con otros) del tratamiento de tales datos. Sin embargo, esta formulación no se mantuvo en el texto final y la experiencia demuestra, por una parte, que el acceso a los datos no implica en sí un control y, por otra, que el acceso a los datos no es una condición esencial para ser responsable del tratamiento. Por ello, en sistemas complejos con varios agentes el acceso a datos personales y otros derechos de los interesados pueden ser garantizados por distintos agentes a diferentes niveles.

Las consecuencias jurídicas también se refieren a la responsabilidad de los responsables del tratamiento y suscitan en particular la pregunta de si el «control conjunto» establecido en la Directiva implica siempre una responsabilidad solidaria. El artículo 23, referido a la responsabilidad, utiliza el singular «responsable del tratamiento» y, por tanto, apunta hacia una respuesta positiva. Sin embargo, como ya se ha señalado, la

¹⁷ Para mayor información y ejemplos, véase el dictamen 5/2009 del Grupo del Artículo 29 sobre las redes sociales en línea, adoptado el 12 de junio de 2009 (WP 163).

realidad puede ofrecer varias vías para actuar «conjuntamente con», es decir «junto con». Esto puede llevar en ciertas circunstancias a una responsabilidad solidaria, aunque no necesariamente: en muchos casos, los distintos responsables del tratamiento pueden tener la responsabilidad —y, por tanto, deben responder— del tratamiento de datos en distintas fases y en distintos grados.

El corolario es que debe garantizarse que, incluso en entornos complejos de tratamiento de datos en los que distintos responsables desempeñen un papel en el tratamiento de datos personales, el cumplimiento de las normas de protección de datos y la responsabilidad de posibles infracciones de tales normas estén claramente asignados a fin de evitar que la protección de datos personales se vea mermada o que se produzca un «conflicto negativo de competencia» o lagunas por las que ciertas obligaciones o derechos emanados de la Directiva no estén garantizados por ninguna de las partes.

En tales casos es más importante aún si cabe que se proporcione a los interesados información escrita en la que se expongan las distintas fases y agentes del tratamiento. Además, debe hacerse constar si cada uno de los responsables del tratamiento tiene la competencia para velar por el respeto de todos los derechos de los interesados o cuál es en cada caso el responsable competente de los distintos derechos.

Ejemplo nº 13: Bancos y bases de datos de clientes morosos

Varios bancos pueden crear una base de datos común —si la legislación nacional lo permite— en la que cada uno introduce información (datos) sobre clientes morosos y a partir de la cual todos pueden acceder a toda la información almacenada. Algunas legislaciones establecen que las solicitudes de los interesados, por ejemplo para pedir el acceso o la supresión de los datos, sólo necesitan cursarse a un «punto de entrada», el proveedor. Corresponde al proveedor localizar al responsable del tratamiento competente y velar por que se den las respuestas pertinentes al interesado. La identidad del proveedor figura publicada en el Registro de Tratamiento de Datos. En otras jurisdicciones, es posible que estas bases de información las gestionen distintos entes legales en tanto que responsables del tratamiento, mientras que las solicitudes para el acceso de los interesados las tramitan los bancos participantes, que actúan como intermediarios.

Ejemplo nº 14: Publicidad orientada por los comportamientos

La publicidad orientada por los comportamientos utiliza información recogida sobre el comportamiento de un individuo cuando navega por internet, como las páginas que visita o las búsquedas que realiza, para seleccionar el tipo de publicidad que se le va a ofrecer. Tanto los editores, que a menudo alquilan espacios de publicidad en sus sitios web, como los proveedores de redes de publicidad, que rellenan esos espacios con publicidad orientada al usuario, pueden recoger e intercambiar información sobre usuarios, en función de los acuerdos contractuales específicos que hayan suscrito.

Desde el punto de vista de la protección de datos, el editor puede considerarse responsable del tratamiento autónomo en la medida en que recoge datos personales del usuario (perfil de usuario, dirección IP, localización, lengua del sistema operativo, etc.) para sus propios fines. El proveedor de redes de publicidad también será responsable del tratamiento en la medida en que determina los fines (seguimiento de los usuarios a través de los sitios web) o los medios esenciales del tratamiento de datos. Dependiendo de las condiciones de la colaboración entre el editor y el proveedor de redes de publicidad —por ejemplo, si el editor permite la transferencia de datos personales al proveedor, incluso redireccionando al usuario a la página web del proveedor—, podría considerarse que ambos son conjuntamente responsables del tratamiento del conjunto de operaciones de tratamiento que dan lugar a la publicidad orientada por los comportamientos.

En todos los casos, los responsables (de forma conjunta) del tratamiento deben garantizar que la complejidad y las características técnicas del sistema de publicidad orientada por el comportamiento no les impidan encontrar las vías adecuadas para cumplir con las obligaciones que incumben a los responsables del tratamiento y salvaguardar los derechos de los interesados. Esto se refiere en particular a:

- la *información* al usuario sobre el hecho de que sus datos son accesibles a un tercero: esto lo podría hacer de manera más eficaz el editor, que es el principal interlocutor del usuario;
- y las condiciones del *acceso* a los datos personales: la empresa de redes de publicidad debería responder a las preguntas de los usuarios sobre la manera en que realizan la publicidad orientada en función de los datos de los usuarios, y cómo atienden las solicitudes de corrección y supresión.

Además, los editores y los proveedores de redes de publicidad pueden estar sujetos a otras obligaciones emanadas de la legislación civil y de protección de los consumidores, incluido el Derecho de daños y las prácticas comerciales desleales.

Conclusión preliminar

Las partes que actúan conjuntamente tienen un cierto grado de flexibilidad a la hora de asignar y repartirse las obligaciones y responsabilidades, siempre y cuando velen por su pleno cumplimiento. Las normas sobre cómo ejercer las responsabilidades compartidas las deben determinar, en principio, los responsables del tratamiento. Ahora bien, también en este caso deberían tomarse en consideración las circunstancias de hecho, a fin de evaluar si el reparto refleja la realidad del tratamiento de datos subyacente.

Desde esta óptica, la evaluación del control conjunto ha de tener en cuenta, por un lado, la necesidad de garantizar el pleno cumplimiento de las normas de protección de datos y, por otro, que la multiplicación de responsables del tratamiento también puede dar lugar a

complejidades indeseadas y a una posible falta de claridad en la atribución de responsabilidades. Se correría entonces el riesgo de convertir en ilícito todo el tratamiento debido a la falta de transparencia y se violaría el principio de tratamiento justo.

Ejemplo nº 15: Plataformas de gestión de datos sanitarios

En un Estado miembro, una autoridad pública crea un punto nacional para el intercambio de datos sobre pacientes entre prestadores de servicios sanitarios. La gran cantidad de responsables del tratamiento —decenas de miles— genera una situación tan poco clara para los interesados (los pacientes) que la protección de sus derechos corre peligro. De hecho, para los interesados no estaría claro a quién dirigirse en caso de queja, pregunta o solicitud de información o para pedir una corrección o el acceso a datos personales. Además, la autoridad pública es responsable de la concepción del tratamiento y del modo en que se utiliza. Estos elementos llevan a la conclusión de que la autoridad pública que establece el punto de intercambio de información debe considerarse responsable del tratamiento conjunto, así como punto de contacto para las solicitudes de los interesados.

Habida cuenta de estas circunstancias, cabe argumentar que la responsabilidad solidaria de todas las partes implicadas debe considerarse un medio para eliminar incertidumbres y, en consecuencia, sólo debe presumirse que existe tal responsabilidad solidaria cuando las partes implicadas no hayan establecido una asignación alternativa, clara e igualmente eficaz de las obligaciones y responsabilidades o cuando ésta no emane claramente de las circunstancias de hecho.

III.2. Definición del encargado del tratamiento

El concepto de encargado del tratamiento no figuraba en el Convenio 108. La función del encargado del tratamiento se reconocía por primera vez en la primera propuesta de la Comisión —aunque ésta no introducía el concepto— con el fin de «evitar situaciones en las que el tratamiento por terceros por cuenta del responsable del tratamiento del fichero tenga el efecto de reducir el nivel de protección del que goza el interesado». El concepto de encargado del tratamiento sólo se recoge explícita y autónomamente en la propuesta modificada de la Comisión y después de una propuesta del Parlamento Europeo cuando, antes de revestir su formulación actual en la Posición Común del Consejo.

Al igual que la definición del responsable del tratamiento, la definición del encargado del tratamiento abarca una amplia variedad de agentes que pueden desempeñar ese papel («persona física o jurídica, autoridad pública, servicio o cualquier otro organismo»).

La existencia de un encargado del tratamiento depende de una decisión adoptada por el responsable del tratamiento, que puede decidir que los datos se traten dentro de su organización, por ejemplo por personal autorizado para procesar datos bajo su autoridad directa (véase, en sentido inverso, el artículo 2.f)), o delegar todas o una parte de las actividades de tratamiento en una organización externa, es decir —como se señala en la exposición de motivos de la propuesta modificada de la Comisión—, en «una persona jurídicamente distinta que actúa por su cuenta».

Por lo tanto, para poder actuar como encargado del tratamiento tienen que darse dos condiciones básicas: por una parte, ser una entidad jurídica independiente del responsable del tratamiento y, por otra, realizar el tratamiento de datos personales por cuenta de éste.

Esta actividad de tratamiento puede limitarse a una tarea o contexto muy específicos o ser más general y amplia.

Además, la función de encargado del tratamiento no se deriva de la naturaleza de un ente que trata datos, sino de sus actividades concretas en un contexto específico. En otras palabras, un mismo ente puede actuar a la vez como responsable del tratamiento para determinadas operaciones de tratamiento y como encargado del tratamiento para otras, y la condición de responsable o encargado debe evaluarse respecto de unos conjuntos muy determinados de datos u operaciones.

Ejemplo nº 16: Proveedores de servicios de alojamiento de datos en internet

Un ISP que presta servicios de alojamiento de datos es, en principio, un encargado del tratamiento de datos personales publicados en línea por sus clientes, que utilizan este ISP para el alojamiento y mantenimiento de su sitio web. Ahora bien, si el ISP somete los datos contenidos en el sitio web a un tratamiento adicional para sus propios fines, se convierte en responsable del tratamiento de los datos en lo relativo a ese tratamiento específico. Este análisis es distinto al de un ISP que presta servicios de correo electrónico o de acceso a internet (véase también el ejemplo nº 1: operadores de telecomunicaciones).

El elemento más importante es el que establece que el encargado del tratamiento actúa «por cuenta del responsable del tratamiento». Actuar en nombre de alguien significa servir los intereses de otro y remite al concepto legal de «delegación». En el caso de la normativa de protección de datos, el encargado del tratamiento está llamado a aplicar las instrucciones dadas por el responsable del tratamiento, cuando menos en lo relativo a los fines del tratamiento y a los elementos esenciales de los medios.

Desde esta óptica, la legitimidad de la actividad de tratamiento del encargado del tratamiento de los datos viene determinada por el mandato conferido por el responsable del tratamiento. Un encargado del tratamiento que va más allá de su mandato y desempeña una función importante en la determinación de los fines o los medios esenciales del tratamiento actúa como responsable (conjuntamente con otros) más que como encargado del tratamiento. La cuestión de la legitimidad de este tratamiento se evaluará a la luz de otros artículos (6 a 8). Ahora bien, la delegación aún puede implicar un cierto grado de discrecionalidad sobre cómo servir mejor los intereses del responsable del tratamiento, permitiendo que el encargado del tratamiento elija los medios técnicos y de organización más adecuados.

Ejemplo nº 17: Externalización de servicios de correo

Unos entes privados prestan servicios de correo por cuenta de agencias (públicas); por ejemplo, la correspondencia relativa a los permisos familiares y de maternidad por cuenta de la Agencia Nacional de la Seguridad Social. En este caso, una autoridad de protección de datos señaló que los entes privados en cuestión debían considerarse encargados del tratamiento dado que su cometido, a pesar de realizarse con un cierto grado de autonomía, se limitaba a sólo una parte de las operaciones de tratamiento necesarias para los fines determinados por el responsable del tratamiento de los datos.

Con el mismo objeto de velar por que la externalización y delegación no den lugar a una disminución del nivel de protección de datos, la Directiva contiene dos disposiciones específicamente dirigidas al encargado del tratamiento y que definen con gran detalle sus obligaciones en materia de confidencialidad y seguridad.

- El artículo 16 establece que el propio encargado del tratamiento, así como las personas que actúen bajo su autoridad, sólo podrán tratar datos personales a los que tengan acceso cuando se lo encargue el responsable del tratamiento.

- El artículo 17, relativo a la seguridad del tratamiento, establece la necesidad de que haya un contrato u otro acto jurídico vinculante que regule la relación entre el responsable y el encargado del tratamiento de datos. Dicho contrato debe constar por escrito a efectos de conservación de la prueba y ha de tener un contenido mínimo que establezca, en particular, que el encargado del tratamiento sólo actúa siguiendo instrucciones del responsable del tratamiento y contemple medidas técnicas y de organización para proteger adecuadamente los datos personales. El contrato debe contener una descripción suficientemente detallada del mandato del encargado del tratamiento.

A este respecto debe señalarse que, en muchos casos, los proveedores de servicios especializados en ciertos tipos de tratamiento de datos (por ejemplo, nóminas de asalariados) elaborarán servicios y contratos tipo que se someterán a la firma de los responsables del tratamiento y que, *de facto*, establecerán un modo estándar de tratar los datos personales¹⁸. No obstante, el hecho de que el contrato y sus condiciones detalladas las elabore el proveedor del servicio y no el responsable del tratamiento no es *por sí mismo* base suficiente para concluir que el proveedor del servicio deba considerarse el responsable del tratamiento, en la medida en que el responsable ha aceptado libremente las condiciones contractuales y, por lo tanto, la plena responsabilidad sobre éstas.

En la misma línea, el desequilibrio en cuanto al poder contractual entre un pequeño responsable del tratamiento y un gran proveedor de servicios no debería considerarse una justificación para que el primero acepte cláusulas y condiciones de contratos que no se ajusten a la legislación en materia de protección de datos.

Ejemplo nº 18: Plataformas de correo electrónico

Juan García busca una plataforma de correo electrónico que puedan usar él mismo y los cinco empleados de su empresa. Descubre que una plataforma adecuada y de fácil uso —además de ser la única que se ofrece gratuitamente— conserva los datos personales durante un período excesivo y los transfiere a terceros países sin las salvaguardias apropiadas. Además, las condiciones contractuales son del tipo «o lo tomas o lo dejas».

En este caso, el Sr. García debería buscar a otro proveedor o —en caso de presunto incumplimiento de las normas de protección de datos o de ausencia en el mercado de otros proveedores apropiados— remitir el asunto a las autoridades competentes, como la autoridad de protección de datos, el servicio de defensa de los consumidores, las autoridades antimonopolio, etc.

¹⁸ La elaboración de las condiciones del contrato por el proveedor del servicio no prejuzga el hecho de que los aspectos esenciales del tratamiento, descritos en la letra b) del apartado III.1, sean determinados por el responsable del tratamiento.

El hecho de que la Directiva exija un contrato por escrito para garantizar la seguridad del tratamiento no significa que no pueda haber relaciones entre responsable y encargado del tratamiento sin contrato previo. Desde este punto de vista, el contrato no es constitutivo ni decisivo, si bien puede ayudar a que se entiendan mejor las relaciones entre las partes¹⁹. Por lo tanto, en este caso también debe adoptarse un enfoque funcional que analice los elementos de hecho de las relaciones entre los distintos interesados y la manera en que se determinan los fines y medios del tratamiento. En el supuesto de que exista una relación responsable/encargado del tratamiento, estas partes tienen la obligación de concluir un contrato con arreglo a la legislación vigente (cf. el artículo 17 de la Directiva).

Pluralidad de encargados del tratamiento

Ocurre cada vez con mayor frecuencia que el responsable externalice el tratamiento de datos personales a varios encargados del tratamiento. Estos encargados del tratamiento pueden tener una relación directa con el responsable del tratamiento de los datos o ser subcontratistas en los que los encargados han delegado parte de las actividades de tratamiento que les hayan sido atribuidas.

Estas estructuras complejas (de distintos niveles o difusas) de tratamiento de datos personales van en aumento con las nuevas tecnologías y algunas legislaciones nacionales las contemplan explícitamente. No hay nada en la Directiva que impida que, por exigencias organizativas, se pueda designar a varias entidades como encargadas (o subencargadas) del tratamiento de datos, incluso subdividiendo los cometidos en cuestión. Ahora bien, todas ellas tienen que ajustarse a las instrucciones dadas por el responsable del tratamiento de los datos al llevar a cabo el tratamiento.

Ejemplo nº 19: Informática en malla (*grid*)

Las grandes infraestructuras de investigación recurren cada vez más a sistemas informáticos distribuidos, especialmente sistemas en malla, para alcanzar una mayor capacidad de computación y almacenamiento. La informática en malla se instala en distintas infraestructuras de investigación establecidas en diferentes países. Un sistema europeo de informática en malla podría, por ejemplo, consistir en mallas nacionales que, a su vez, estuvieran bajo la responsabilidad de un organismo nacional. Sin embargo, esta malla europea podría no contar con un organismo central responsable de su funcionamiento. Los investigadores que usan una malla de este tipo no suelen saber dónde exactamente se tratan sus datos ni, por tanto, quién es el encargado del tratamiento de datos competente (la situación se complica aún más si hay infraestructuras informáticas en malla en terceros países). Si una infraestructura en malla utiliza los datos de una forma no autorizada, la parte en cuestión podría considerarse responsable del tratamiento si no actúa por cuenta de los investigadores.

¹⁹ No obstante, en algunos casos la existencia de un contrato por escrito puede constituir una condición necesaria para ser automáticamente considerado el responsable del tratamiento en determinados contextos. En España, por ejemplo, el informe sobre los centros de atención telefónica define como encargados del tratamiento a todos los centros de atención telefónica de terceros países, siempre que cumplan lo establecido en el contrato. Este es el caso incluso cuando el contrato ha sido redactado por el encargado del tratamiento y el responsable del tratamiento simplemente lo «suscribe».

El elemento estratégico aquí es que, al haber varios agentes implicados en el proceso, las obligaciones y responsabilidades resultantes de la legislación sobre protección de datos deberían asignarse con claridad y no dispersarse a lo largo de la cadena de externalización o subcontratación. En otras palabras, debería evitarse una cadena de (sub)encargados del tratamiento que diluya o incluso impida un control efectivo y una responsabilidad clara sobre las actividades de tratamiento, a no ser que las responsabilidades de las distintas partes de la cadena estén claramente establecidas.

Desde este punto de vista, y en el mismo sentido de lo expuesto en la letra b) del apartado III.1, si bien no es necesario que el responsable del tratamiento defina y dé su consentimiento a todos los detalles de los medios que van a usarse para perseguir los fines previstos, sí es necesario que al menos esté informado de los elementos principales de la estructura del tratamiento (por ejemplo, partes implicadas, medidas de seguridad, garantías para el tratamiento en terceros países, etc.) a fin de que esté en condiciones de mantener un control sobre los datos que se procesan por su cuenta.

También debe considerarse que, aunque la Directiva impone una responsabilidad al responsable del tratamiento, no impide que las normas nacionales de protección de datos establezcan además que el encargado del tratamiento también deba responder en determinados casos.

Hay una serie de criterios que pueden ser de utilidad para determinar la condición de las distintas partes implicadas:

- Nivel de instrucciones anteriores dadas por el responsable del tratamiento de datos, que determina el margen de maniobra que se deja al encargado del tratamiento de datos.
- Seguimiento por el responsable del tratamiento de datos de la ejecución del servicio. Una supervisión constante y atenta por parte del responsable del tratamiento para garantizar que el encargado del tratamiento cumple debidamente las instrucciones y condiciones del contrato proporciona una indicación de que el responsable del tratamiento sigue teniendo el control pleno y exclusivo de las operaciones de tratamiento.
- Visibilidad/imagen dada por el responsable del tratamiento a los interesados, y expectativas de estos sobre la base de tal visibilidad.

Ejemplo nº 20: Centros de atención telefónica

Un responsable del tratamiento de datos externaliza algunas de sus operaciones a un centro de atención telefónica y le encarga que cuando llame a sus clientes se presente utilizando la identidad del responsable del tratamiento. En este caso, las expectativas de los clientes y la forma en que el responsable del tratamiento se presenta a sus clientes por medio de la empresa encargada de las actividades externalizadas llevan a la conclusión de que dicha empresa actúa como encargada del tratamiento (por cuenta) del responsable del tratamiento.

- Conocimientos especializados de las partes: en algunos casos, la función tradicional y los conocimientos profesionales del proveedor de servicios desempeñan un papel predominante, que puede traer consigo su condición de responsable del tratamiento de datos

Ejemplo nº 21: Representantes procesales

Un representante procesal representa a su cliente ante los tribunales y, en el marco de esa función, trata datos personales relacionados con el caso de su cliente. El fundamento jurídico para utilizar la información necesaria radica en el mandato del cliente. Sin embargo, este mandato no está centrado en el tratamiento de datos, sino en la representación ante los tribunales, actividad para la cuales estas profesiones tradicionalmente cuentan con su propia base jurídica. Por lo tanto, estos profesionales deben considerarse «responsables del tratamiento» independientes cuando tratan datos en el marco de la representación legal de sus clientes.

En un contexto diferente, también puede resultar determinante una evaluación más detallada de los medios establecidos para alcanzar los fines.

Ejemplo nº 22: Sitio web de «objetos perdidos»

Un sitio web de «objetos perdidos» fue presentado como mero encargado del tratamiento por considerarse que corresponde a las personas que publican un anuncio de un objeto perdido determinar el contenido y por tanto, a micronivel, el fin (por ejemplo, recuperar un broche, un loro, etc.) Una autoridad de protección de datos rechazó este argumento. El sitio web se creó con el fin comercial de ganar dinero procedente de la publicación de anuncios de objetos perdidos, y el hecho de que los impulsores no determinaran qué objetos específicos figuraban en los anuncios (pero sí las categorías de objetos) no era esencial, puesto que la definición de «responsable del tratamiento de datos» no contempla explícitamente la determinación del contenido. El sitio web determina las condiciones de la publicación de anuncios, etc., y es responsable de la propiedad del contenido.

Aunque haya habido una tendencia a identificar en general la externalización como un cometido propio de un encargado del tratamiento, en la actualidad las situaciones y evaluaciones son a menudo mucho más complejas.

Ejemplo n° 23: Contables

La consideración de los contables como responsables del tratamiento puede variar en función del contexto. Cuando prestan servicios al público en general y a pequeños comerciantes sobre la base de instrucciones muy genéricas («Prepare mi declaración fiscal») son responsables del tratamiento de datos, del mismo modo que los abogados cuando actúan en circunstancias similares y por razones idénticas. Sin embargo, si el contable es contratado por una empresa y está sujeto a instrucciones precisas dadas por el contable de plantilla, por ejemplo para realizar una auditoría pormenorizada, entonces será por lo general —si no es un asalariado normal— el encargado del tratamiento, dada la precisión de las instrucciones recibidas y la consiguiente limitación del margen discrecional. Ahora bien, hay una salvedad importante y es que, cuando los contables consideran que han descubierto una práctica irregular que tienen la obligación de notificar, entonces están actuando de manera independiente como responsables del tratamiento debido a las obligaciones profesionales que les incumben.

En ocasiones, la complejidad de las operaciones de tratamiento puede llevar a poner más énfasis en el margen de maniobra de quienes están a cargo del tratamiento de datos personales, por ejemplo cuando el tratamiento conlleva un riesgo particular en lo relativo al derecho a la intimidad. La introducción de nuevos medios de tratamiento puede llevar a que se privilegie la consideración de responsable del tratamiento de datos antes que la de encargado. Estos casos también pueden llevar a una aclaración —y designación del responsable del tratamiento— explícitamente contemplada en la legislación.

Ejemplo n° 24: Tratamiento con fines históricos, científicos y estadísticos

La legislación nacional puede introducir, respecto del tratamiento de datos personales con fines históricos, científicos y estadísticos, la noción de organización intermediaria para designar al organismo a cargo de la transformación de datos no codificados en datos codificados, de modo que el responsable del tratamiento con fines históricos, científicos y estadísticos ya no podría volver a identificar a los interesados a que se refieren los datos.

Si varios responsables de las operaciones iniciales de tratamiento transmiten datos a uno o varios terceros para un tratamiento adicional con fines históricos, científicos y estadísticos, los datos son codificados primero por una organización intermediaria. En este caso, la organización intermediaria puede considerarse responsable del tratamiento con arreglo a normas nacionales específicas y está sujeta a todas las obligaciones resultantes (pertinencia de los datos, información a los interesados, notificación, etc.). Esto se justifica por el hecho de que, cuando se reúnen los datos de distintas fuentes, hay una amenaza particular para la protección de datos, lo que a su vez justifica la responsabilidad que incumbe a la propia organización intermediaria. En consecuencia, ésta no se considera simplemente como encargada del tratamiento, sino plenamente como responsable del tratamiento en virtud de la legislación nacional.

En la misma línea, resulta relevante el poder decisorio autónomo que se deja a las distintas partes implicadas en el tratamiento. El caso de los ensayos clínicos de medicamentos demuestra que la relación entre las empresas patrocinadoras y las entidades externas encargadas de realizar los ensayos depende de la discrecionalidad que se deja a dichas entidades en lo relativo al tratamiento de datos. Esto implica que puede

haber más de un responsable del tratamiento, pero también más de un encargado o persona a cargo del tratamiento.

Ejemplo nº 25: Ensayos clínicos de medicamentos

La empresa farmacéutica XYZ patrocina unos ensayos de medicamentos y selecciona a los centros de ensayos interesados evaluando su elegibilidad e intereses respectivos; establece el protocolo de ensayo, facilita a los centros la orientación necesaria en lo relativo al tratamiento de datos y controla el cumplimiento por parte de los centros del protocolo y de los procedimientos internos respectivos.

Aunque la empresa patrocinadora no recoge ningún tipo de datos directamente, sí recibe los datos de los pacientes recogidos por los centros de ensayos y los somete a distintos tratamientos (evalúa la información contenida en los documentos médicos, recibe datos de reacciones adversas; introduce estos datos en las bases correspondientes; realiza análisis estadísticos para obtener los resultados de los ensayos). El centro de ensayos realiza los ensayos de forma autónoma, si bien ajustándose a las orientaciones dadas por el patrocinador; facilita las notas informativas a los pacientes y obtiene su consentimiento también en lo relativo al tratamiento de sus datos; permite a los colaboradores de la empresa patrocinadora acceder a los documentos médicos originales de los pacientes para realizar actividades de seguimiento; y manipula y se responsabiliza de la custodia de estos documentos. Por ello, en apariencia, las responsabilidades recaen sobre los agentes individuales.

En estas circunstancias, tanto los centros de ensayos como las empresas patrocinadoras adoptan en este caso determinaciones importantes en lo relativo al modo en que se tratan los datos personales relacionados con los ensayos clínicos. En consecuencia, pueden considerarse responsables conjuntos del tratamiento de datos. La relación entre el patrocinador y los centros de ensayos podría interpretarse de manera distinta en aquellos casos en que el patrocinador determina los fines y los elementos esenciales de los medios y al investigador le queda un margen de maniobra muy estrecho.

III.3. Definición de tercero

El concepto de «tercero» no figuraba en el Convenio 108, pero se introdujo en la propuesta modificada de la Comisión a raíz de una enmienda propuesta por el Parlamento Europeo. Según la exposición de motivos, la enmienda se reformuló a fin de dejar claro que el concepto de terceros no incluía a los interesados, ni al responsable del tratamiento, ni a ninguna persona autorizada para tratar los datos bajo la autoridad directa del responsable del tratamiento o por cuenta de éste, como es el caso del encargado del tratamiento. Esto significa que *«personas que trabajan para otra organización, incluso si ésta pertenece al mismo grupo o sociedad de cartera, serán en general terceros»* y, en cambio, *«las filiales de un banco que tratan las cuentas de los clientes bajo la autoridad directa de la sede no serían terceros»*.

La Directiva utiliza el concepto «terceros» de una forma que no es distinta de la forma en que habitualmente se utiliza en Derecho civil, donde el tercero suele ser una persona que no es parte de una entidad o acuerdo. En el contexto de la protección de datos, este concepto debería interpretarse como referente a cualquier persona que no tenga legitimidad o autorización específica —como la que emanaría, por ejemplo, de su función de responsable del tratamiento, encargado del tratamiento o sus empleados— para tratar datos personales.

La Directiva utiliza este concepto en muchas disposiciones, en general con vistas a establecer prohibiciones, limitaciones y obligaciones para aquellos supuestos en que los datos personales puedan ser tratados por otras partes que, en principio, no estaba previsto que trataran determinados datos personales.

En estas circunstancias cabe concluir que un tercero que recibe datos personales —ya sea de forma legítima o ilegítima— es, en principio, un nuevo responsable del tratamiento, siempre que se reúnan las demás condiciones para que dicho tercero pueda considerarse responsable del tratamiento y para la aplicación de la normativa sobre protección de datos.

Ejemplo nº 26: Acceso no autorizado de un empleado

Un empleado de una empresa tiene conocimiento, en el ejercicio de sus cometidos, de unos datos personales para los que no tenía autorización de acceso. En este caso, el empleado se consideraría «tercero» respecto de su empleador, con todas las consecuencias y responsabilidades resultantes en términos de legitimidad de la comunicación y el tratamiento de datos.

IV. Conclusiones

El concepto de «responsable del tratamiento» y su interacción con el concepto de «encargado del tratamiento» desempeñan un papel fundamental en la aplicación de la Directiva 95/46/CE, puesto que determinan quién debe ser responsable del cumplimiento de las normas de protección de datos, cómo pueden ejercer sus derechos los interesados, cuál es la legislación nacional aplicable y con qué eficacia pueden operar las autoridades de protección de datos.

Las diferencias de organización en los sectores público y privado, el desarrollo de las TIC y la globalización del tratamiento de datos aumentan la complejidad de dicho tratamiento y requieren una aclaración de estos conceptos con objeto de garantizar una aplicación eficaz y el cumplimiento en la práctica.

El concepto de responsable del tratamiento es autónomo, en el sentido de que debe interpretarse fundamentalmente con arreglo a la legislación comunitaria de protección de datos, y funcional, en el sentido de que su objetivo es asignar responsabilidades en función de la capacidad de influencia de hecho, y, por consiguiente, se basa en un análisis de los hechos más que en un análisis formal.

La definición de la Directiva consta de tres componentes fundamentales: el aspecto personal («*la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo*»); la posibilidad de un control plural («*que solo o conjuntamente con otros*»); los elementos esenciales para distinguir al responsable del tratamiento de otros agentes («*determine los fines y los medios del tratamiento de datos personales*»).

El análisis de estos componentes conduce a los siguientes resultados principales:

- La capacidad de «*determinar los fines y los medios*» puede emanar de distintas circunstancias jurídicas y/o de hecho: una competencia legal explícita, cuando la legislación establece el nombramiento del responsable del tratamiento o dispone el

cometido o la obligación de recoger y tratar determinados datos; normas jurídicas generales o funciones tradicionales existentes que, por lo común, implican una determinada responsabilidad dentro de determinadas organizaciones (por ejemplo, el empleador en relación con los datos sobre sus empleados); circunstancias de hecho y otros elementos (como las relaciones contractuales, el control real ejercido por una parte, la visibilidad de cara a los interesados, etc.).

Si no cabe aplicar ninguna de las categorías mencionadas, el nombramiento de un responsable del tratamiento debe considerarse nulo de pleno derecho. Por eso, un organismo que no tenga capacidad de influencia de hecho ni de derecho para determinar cómo se tratan los datos personales no puede considerarse responsable del tratamiento.

El hecho de determinar los «fines» del tratamiento trae consigo la consideración de responsable del tratamiento (*de facto*). En cambio, la determinación de los «medios» del procesamiento puede ser delegada por el responsable del tratamiento en la medida en que se trate de cuestiones técnicas u organizativas. Sin embargo, las cuestiones de fondo que sean esenciales a efectos de la legitimidad del tratamiento —como los datos que deban tratarse, la duración de su conservación, el acceso, etc.— deben ser determinadas por el responsable del tratamiento.

- El aspecto *personal* de la definición se refiere a una amplia gama de sujetos que pueden desempeñar la función de responsable del tratamiento. En cambio, desde el punto de vista estratégico de la asignación de responsabilidades, preferentemente debe considerarse responsable del tratamiento a la empresa o al organismo como tal, antes que a una persona concreta dentro de la empresa o el organismo. En última instancia, debe considerarse responsable del tratamiento de datos y de las obligaciones que emanan de la legislación de protección de datos a la empresa o al organismo, a no ser que haya elementos inequívocos que indiquen que el responsable debe ser una persona física, por ejemplo cuando una persona física que trabaja en una empresa u organismo público utiliza los datos para sus propios fines, al margen de las actividades de la empresa.
- La posibilidad de un *control plural* responde al número creciente de situaciones en que diferentes partes actúan como responsables del tratamiento. La evaluación de este control conjunto debería ser un reflejo de la evaluación del control «único», adoptando un enfoque sustantivo y funcional centrado en establecer si los fines y los aspectos esenciales de los medios los determina más de una parte.

La participación de las partes en la determinación de los fines y los medios del tratamiento en el contexto del control conjunto puede revestir distintas formas y el reparto no tiene que ser necesariamente a partes iguales. El presente dictamen proporciona muchos ejemplos de distintos tipos y grados de control conjunto. Los distintos grados de control pueden dar lugar a distintos grados de responsabilidad, y desde luego no cabe presumir que haya una responsabilidad solidaria en todos los casos. Por lo demás, es muy posible que en sistemas complejos con varios agentes el acceso a datos personales y el ejercicio de otros derechos de los interesados también los puedan garantizar distintos agentes a diferentes niveles.

Este dictamen analiza asimismo el concepto de encargado del tratamiento, cuya existencia depende de una decisión adoptada por el responsable del tratamiento, que puede decidir que los datos se traten dentro de su organización o bien delegar todas o una

parte de las actividades de tratamiento a una organización externa. Por lo tanto, para poder actuar como encargado del tratamiento tienen que darse dos condiciones básicas: por una parte, ser una entidad jurídica independiente del responsable del tratamiento y, por otra, realizar el tratamiento de datos personales por cuenta de éste. Esta actividad de tratamiento puede limitarse a una tarea o contexto muy específicos o dejar un cierto grado de discrecionalidad sobre cómo servir los intereses del responsable del tratamiento, permitiendo que el encargado del tratamiento elija los medios técnicos y de organización más adecuados.

Además, la función de encargado del tratamiento no se deriva de la naturaleza de un agente que trata datos personales, sino de sus actividades concretas en un contexto específico y respecto de unos conjuntos muy determinados de datos u operaciones. Hay una serie de criterios que pueden ser de utilidad para determinar la condición de las distintos agentes implicados en el tratamiento: el nivel de instrucciones anteriores dadas por el responsable del tratamiento de datos; el seguimiento por el responsable del tratamiento de datos del nivel del servicio; la visibilidad de cara a los interesados; los conocimientos especializados de las partes; el poder decisorio autónomo que se deja a las distintas partes.

Por fin, la categoría «tercero» se define como cualquier agente que no tenga legitimidad o autorización específica —como la que emanaría, por ejemplo, de su función de responsable del tratamiento, encargado del tratamiento o sus empleados— para tratar datos personales.

* * *

El Grupo reconoce las dificultades para poner en práctica las definiciones de la Directiva en un entorno complejo en el que caben muchas situaciones hipotéticas que impliquen la actuación de responsables y encargados del tratamiento, solos o conjuntamente, y con distintos grados de autonomía y responsabilidad.

En su análisis hace hincapié en la necesidad de asignar la responsabilidad de tal manera que el cumplimiento de las normas de protección de datos se vea suficientemente garantizado en la práctica. Con todo, no ha encontrado razón alguna para considerar que la distinción actual entre responsables y encargados del tratamiento ya no sea pertinente y viable desde esta perspectiva.

Por ello, el Grupo espera que las explicaciones dadas en su dictamen, ilustradas con ejemplos concretos tomados de la experiencia cotidiana de las autoridades de protección de datos, sirvan de orientación sobre cómo interpretar estas definiciones esenciales de la Directiva.

Bruselas, 16 de febrero de 2010

Por el Grupo
El Presidente
Jacob KOHNSTAMM