Universidad Internacional de La Rioja

Facultad de Derecho

Máster Universitario en Protección de Datos

Flujos de datos entre grupos de empresas

Trabajo fin de estudio presentado por:	María José Melón Baena
Tipo de trabajo:	Trabajo de Fin de Máster
Directora:	María Elena Salgado André
Fecha:	16 de julio de 2020

Resumen

El objeto de este estudio es analizar el tratamiento de los datos personales que se lleva a cabo en determinados grupos de empresas en los que la estructura societaria está muy centralizada, de tal modo que todos los procesos los controla la matriz y las filiales son meramente sociedades vehículo. Mientras la norma (y el criterio interpretativo de la AEPD) obligan a que cada sociedad del grupo aplique de forma independiente e individualizada la normativa de protección de datos, la realidad es que multitud de procesos son únicos para el grupo y en muchos casos no encuentran acomodo sencillo en los esquemas existentes para el intercambio de datos personales. Con la regulación actual, el consentimiento ya no es criterio principal para efectuar cesiones de datos; si bien esta mayor libertad para el responsable del tratamiento viene acompañada de un estándar más elevado a la hora de informar a los interesados. La cuestión es si con la regulación actual se podría simplificar la estructura de gestión de esos flujos de datos al mismo tiempo que facilitar una información clara y sencilla al interesado para que realmente comprenda quién y cómo está tratando sus datos.

Palabras clave: (grupos de empresa; uso datos de terceros; transparencia en las cesiones; flujo de datos intragrupo; RGPD)

Abstract

The purpose of this study is to analyze the treatment of personal data. vehicle. While the norm (and the interpretative criteria of the AEPD) requires each group company to apply the data protection regulations independently and individually, the reality is that many processes are unique to the group and in many cases not They find simple accommodation in complex schemes for exchanging personal data. With the current regulation, consent is no longer the main criterion for correcting data transfers; although this greater freedom for the controller is accompanied by a higher standard when informing those interested. The question is whether under current regulation you could simplify the management structure for those data changes while providing clear and simple information to the data subject so that they really understand who and how they are handling their data.

Key words: (company groups; use of third-party data, transparency in the transfers; RGPD).

Índice de contenidos

1. Introducción

La evolución del principio de transparencia desde la *Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*, hasta el *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos* (en adelante "RGPD"), ha supuesto un cambio notable en la forma de proporcionar información a los interesados en relación con el tratamiento de sus datos personales. El cambio principal reside en la exhaustividad con la que se ha de facilitar la información, y objetivo primordial perseguido viene siendo incrementar la transparencia para que el interesado pueda conocer y decidir con criterio si quiere que sus datos sean tratados o no. En definitiva, se trata de incrementar la capacidad de control de los interesados sobre el uso que los terceros hacen de sus datos personales.

La Directiva establecía el mínimo de información exigible de forma somera, sin apenas indicar el grado de detalle de la información a suministrar. De hecho, la Directiva establecía con carácter imperativo indicar (i) la identidad del responsable del tratamiento y, en su caso, de su representante; y, (ii) los fines del tratamiento en términos genéricos. Con carácter suplementario, y admitiendo un margen de subjetividad, se indicaba que, además, se facilitaría cualquier otra información que resultara necesaria para garantizar un tratamiento de datos leal respecto del interesado.

El RGPD profundiza mucho más en la obligación de proporcionar información, como parte de la expresión el principio de tratamiento leal y transparente. Así, regula expresamente: (i) cuándo se debe informar (eliminando toda excepción y con independencia de la base de legitimación sobre la que se funde el tratamiento); (ii) el contenido y detalle que se debe proporcionar al interesado (destaca, en particular, la obligación de informar del plazo durante el cual van a conservarse los datos personales); y, (iii) el modo en que se debe facilitar dicha información (de forma clara y fácilmente comprensible por el público al que va destinada).

Y, como más adelante se indicará, regula con la misma exhaustividad la información a facilitar cuando los datos han sido obtenidos de una fuente distinta del propio interesado.

Esta cuestión en concreto supone un cambio muy relevante, que no ha gozado de mucha publicidad, ni en los currículos de estudio ni, aparentemente, en la doctrina. Se trata, no obstante, de un cambio sustancial muy relevante que afecta de lleno al supuesto de hecho cuyo análisis es objeto de este trabajo.

1.1. Justificación del tema elegido

La articulación de los flujos de datos dentro de un grupo de empresas no es una cuestión sencilla ni baladí. En función del flujo existente y de la estructura del grupo variará el análisis teórico de las diferentes maneras de articular las relaciones intragrupo en lo que al flujo de datos personales se refiere. Las consecuencias prácticas que de cada esquema se pueden derivar son el objeto de este estudio. Más concretamente, se centrará en un supuesto muy concreto de determinados grupos de empresas: aquellos en los que, de facto, de cara al cliente, existe un único negocio y una única imagen corporativa. A los efectos del presente documento y para facilitar la lectura del mismo me referiré a ellos en lo sucesivo bajo el nombre genérico de "Grupos de Empresas".

1.2. Problema y finalidad del trabajo

Es criterio asentado de la Agencia Española de Protección de Datos (en adelante "AEPD") todas las sociedades pertenecientes a un mismo grupo de empresas deben mantener diferenciada su personalidad jurídica y ello supone que cada sociedad debe dar cumplimiento íntegro e independiente del resto de las sociedades de ese mismo grupo a la normativa de protección de datos personales (Informe 0245, Gabinete Jurídico. AEPD. 2010). Ello, con independencia de las características del grupo de empresas. Pero la realidad es que, en los Grupos de Empresa, todos los flujos de las filiales no son sino un único tratamiento realizado por o en colaboración con la matriz. La determinación del mecanismo de articulación del uso intragrupo de los datos (encargo de tratamiento, esquema de corresponsabilidad o cesión, básicamente) tiene efectos en otras áreas del derecho y, evidentemente, en la información a trasladar al interesado, lo que puede llegar a ser más complejo de lo que parecería en un primer análisis y supone un incremento notable de la burocracia que, acaso, sea innecesario o cuando menos, poco eficiente.

1.3. Objetivos

En definitiva, aquí se abordarán las diferentes posibilidades que ofrece la normativa en cuanto al tratamiento de datos dentro de los Grupos de Empresa, con especial atención a la forma de articular las cesiones de datos y determinar la mejor alternativa posible atendiendo a criterios de practicidad dentro de la normativa aplicable y buscar posibles alternativas más eficientes pero garantistas con los principios del RGPD. El enfoque del estudio es eminentemente práctico, siendo este un aspecto que, a menudo, es olvidado por el legislador, especialmente cuando se trata de entidades con menor capacidad de asunción de estructuras formales de gestión de procesos internos (empresas medianas con recursos humanos y tecnológicos limitados). La norma aborda los problemas más relevantes y se deja para la interpretación jurisprudencial (y administrativa —en este caso de la AEPD—), la gestión de las dificultades y discrepancias que surgen en la práctica al implementar la norma en sujetos obligados que, por su escasa relevancia en volumen y actividad, no están en la primera línea del pensamiento del legislador.

2. Descripción detallada del supuesto de hecho

Con carácter general, y salvo en el ámbito de las actividades reguladas, toda persona tiene libertad para llevar a cabo una actividad comercial, pudiendo organizarla del modo que mejor convenga a sus intereses, existiendo múltiples figuras a tal fin, cada una con un régimen y particularidades propias. La figura más empleada por excelencia es la sociedad mercantil, ya sea en su modalidad de sociedad limitada o de sociedad anónima; y ello, por la separación que se genera respecto del patrimonio personal del accionista. A medida que estas sociedades se consolidan y empiezan a crecer, abordando nuevas actividades dentro de la misma línea de negocio (que no necesariamente nuevos negocios) es frecuente que busquen una nueva separación patrimonial respecto de la empresa original ya consolidada, mitigando así los riesgos en caso de que la nueva actividad no llegue a fructificar. En otros casos, la empresa se constituye desde un inicio como un conjunto de varias entidades participadas íntegramente por la matriz al objeto de desarrollar partes concretas de un negocio, por una mera cuestión fiscal vinculada al cumplimiento de la normativa tributaria y la obligación de dar de alta cada actividad en un epígrafe determinado del Impuesto de Actividades Económicas. Sería este, por ejemplo, el caso de un propietario de terrenos en los que desarrolla y opera conjuntamente un negocio de promoción inmobiliaria, otro de gestión de campo de golf y, finalmente, un área de restauración; el negocio es uno, pero se ofertan productos y servicios que fiscalmente corresponden a diferentes epígrafes y lo normal será estructurar el negocio a través de tantas sociedades como actividades fiscales diferentes, por el impacto que esta decisión tiene en otros impuestos tales como el Impuesto sobre el Valor Añadido. Es decir, por motivos fiscales y de limitación de responsabilidad las empresas, los negocios tienden a estructurarse en grupos de empresas. Con carácter general, ello supondría replicar la estructura burocrática de cada entidad independiente dentro del grupo de empresas; y, sin embargo, en cada disciplina del Derecho se tiende a reconocer y regular (con distintos grados de intensidad) las consecuencias de la existencia de los grupos de empresa para evitar ineficiencias.

Así, en primer lugar, encontramos la legislación propiamente mercantil y contable, de donde nace la definición de grupo de empresa (art. 42 CCo) y ya desde ese mismo momento en que se reconoce la existencia de grupos de empresas se regula cómo debe procederse a efectos contables (y, por lo tanto, fiscales) con carácter general cuando existe una unidad de

decisión, existirá un grupo de empresas. En las disciplinas de Precios de Transferencia, Derecho Laboral, Derecho de la Competencia, Contratación Pública, Prevención del Blanqueo de Capitales, por citar una pocas, se reconoce y regula expresamente la aplicación de la norma objeto de cada disciplina a los grupos de empresa, reconociendo especificidades propias, normalmente para evitar el fraude en el cumplimiento de la norma o simplemente para evitar generar ineficiencias.

En el ámbito de la Protección de Datos, el legislador solo ha dado carta de naturaleza a los grupos de empresa a la hora de regular las transferencias internacionales, reconociendo y dando luz verde a las transferencias internacionales realizadas en el seno de grupos de empresa que cuenten con normas corporativas vinculantes. El legislador en ningún momento ha contemplado la posibilidad de que los grupos de empresa puedan dar cumplimiento a la normativa de protección de datos a nivel de grupo; aun si los tratamientos que realizan son prácticamente idénticos, las políticas y protocolos establecidos en cada empresa del grupo son los mismos y de cara al mercado existe una unidad de decisión y de acción. En palabras de VALDIVIESO LÓPEZ, E. (2012), "*la aparición de los grupos de empresas [.....] requiere de un marco legal adecuado que pueda responder a las necesidades de este nuevo tipo de configuración empresarial, no sólo desde el punto de vista societario o empresarial, sino desde otros aspectos jurídicos involucrados, como el tributario, civil, constitucional o laboral*".

Desde luego, en materia de protección de datos podría ser muy recomendable el establecimiento de un cuerpo legal regulatorio a nivel de grupo. Sin embargo, la realidad es que, en ausencia de norma que regule la cuestión, el criterio de la AEPD es claro: cada sociedad pertenezca o no a un grupo de empresas, debe dar cumplimiento a la normativa de protección de datos. Dicho razonamiento se encuentra recogido en el fundamente de derecho cuarto de la de la Sección Novena de la Sala de lo Contencioso-administrativo del Tribunal Superior de Justicia de Madrid, de 16 de octubre de 2000 (nº 848/2000, rec. 1132/1997; EDJ 2000/112449) que indica que: "*Cualquier empresa es libre de constituirse en cualquiera de las formas societarias que el Derecho Mercantil regula. Asimismo, las empresas pueden unirse a través de las distintas formas reguladas en derecho: fusión, Absorción, etc. Pero, desde luego, lo que no cabe es que existan dos sociedades anónimas y, como tales, independientes y con personalidad jurídica autónoma y que por el hecho de que*

una sea propiedad de la otra, el particular que contrata con la primera pueda verse perjudicado, precisamente, por la estructura empresarial que la sociedad ha elegido. Si la recurrente ha preferido constituir dos sociedades y trabajar con ellas de manera independiente, beneficiándose así del mantenimiento de dos personas jurídicas distintas, no puede, al mismo tiempo, pretender justificar el conocimiento por parte de la matriz de los datos que le constan a la filial por las operaciones que esta última ha intervenido, pues ello supone olvidarse de que se trata de personas jurídicas distintas" (énfasis añadido).

Así pues, se sienta el principio de que, en ausencia de norma, no cabe ampararse en la existencia de un grupo societario para defender la aplicación de la norma como si de una sociedad se trata, pues se optó por constituir varias, con las ventajas que en otros órdenes ello comportaba. Pero en la sentencia citada esta conclusión se vincula al hecho de que la pretensión de aplicación conjunta de la norma de protección de datos al grupo como si de una única empresa se tratara resultarían en perjuicio de tercero.

En este escenario, de aplicación individualiza de la normativa aplicable por cada sociedad dentro de un grupo de empresas, podría no obstante darse la circunstancia de que las filiales quedaran exentas de la aplicación de determinados requisitos normativos, como puede ser la necesidad de contar con un DPO o de llevar un registro de actividades del tratamiento; pensemos por ejemplo en filiales sin empleados. No parece que esto tenga mucho sentido, si la matriz domina los procesos y es una empresa que sí supera los umbrales definidos para la aplicación de estos aspectos normativos.

Volviendo al planteamiento de este trabajo, y con el foco puesto en lo que he denominado Grupos de Empresa, procede, por lo tanto, analizar:

(i) Las alternativas existentes para canalizar los flujos de datos entre compañías del mismo grupo conforme a la normativa de protección de datos; y,
(ii) Si acaso no resultaría en beneficio de tercero la existencia de una regulación que permitiera la aplicación conjunta de la normativa en este tipo de Grupos de Empresa. Evidentemente, esto supone un mero ejercicio dialéctico puesto que tanto la norma como el criterio interpretativo del Tribunal Supremo hoy por hoy son claros y no están controvertidos.

3. Alternativas posibles para el tratamiento de los datos

Aceptado el principio de que cada empresa debe cumplir íntegramente las obligaciones que le incumben en materia de protección de datos de forma independiente de su pertenencia a un grupo de empresas, a priori cabe establecer tres formas diferentes para diseñar el flujo de datos:

(i) el establecimiento de relaciones contractuales para la encomienda de encargos de tratamiento, caso a caso;

(ii) el establecimiento de contratos de corresponsabilidad en aquellos supuestos en que la determinación de los medios y fines del tratamiento sea conjunta o no sea clara la delimitación de responsabilidades a priori; y,

(iii) acudir a la figura de la cesión de datos, recogiendo todos los datos que son objeto de cesión, con las implicaciones y dificultades que ello puede conllevar, especialmente en materia de información al interesado y legitimación del tratamiento.

3.1. Encargo de tratamiento

Quizá sea este el esquema más extendido de regulación de relaciones a efectos de protección de datos en grupos de empresas: una empresa es responsable de los datos que otra procesa por cuenta de este.

3.1.1. Regulación

El encargo de tratamiento encuentra su acomodo legal en el artículo 28 RGPD. Se configura como la prestación, por parte del encargado del tratamiento, de un servicio a favor del responsable del tratamiento, que implica el acceso a determinados datos para poder ser ejecutado. Debe regularse por escrito ya sea de forma anexa o integrada en el propio contrato de prestación de servicios o como documento aparte, pero necesariamente vinculado al de prestación de los servicios para los que el encargo es necesario y detallando todos los aspectos requeridos conforme al artículo 28 RGPD, que es la fuente de esta figura.

La clave para determinar la existencia de un encargo de tratamiento reside en identificar quien tiene la capacidad de decidir sobre los medios y fines del tratamiento (art. 4.7 RGPD). El encargado del tratamiento debe limitarse a cumplir con las instrucciones de quien le encomienda un determinado servicio, estableciendo con sus procesos organizativos y

operacionales propios que sean necesarios para la prestación del servicio, pero pasará a ser considerado responsable del tratamiento si utiliza los datos para sus propios fines. Eso sí, asumiría esta posición por incumplimiento y por lo tanto con riesgo de ser sancionado —art.83.4 RGPD—.

3.1.2. Aplicación práctica

En una primera aproximación parece evidente que la figura del encargo de tratamiento encaja bastante bien con la realidad de los flujos de datos en grupos de empresas centralizadas; en los que los procesos se gestionan normalmente por la matriz, o por una o varias de las empresas del grupo, que presta sus servicios a todas las demás. En estos casos, la regulación de protección de datos es sencilla y no difiere sustancialmente respecto de la normativa anterior a la entrada en vigor del RGPD. En este sentido, se puede apuntar que el RGPD impone obligaciones adicionales al encargado que, con la regulación anterior, no se especificaban como tal (el grueso de las cuales recaen en la aplicación de las medidas de seguridad convenidas con el responsable del tratamiento y, en su caso, la obligación de llevar el registro de actividades de tratamiento y designar un DPO). A pesar de estas nuevas obligaciones, en términos generales, es el esquema más práctico para regular los flujos de datos entre compañías del mismo grupo, entre otras cosas porque, en principio, no existe obligación de informar al interesado sobre la existencia contenido y detalle del encargo del tratamiento, lo cual simplifica la gestión relativa al recabo de datos sin merma de la calidad de la información suministrada al cliente.

Ahora bien; esta afirmación de que no es preciso detallar los encargos de tratamiento en la información suministrada al cliente con carácter previo al recabo de sus datos conviene matizarla. Y es que no faltan autoridades en la materia que defienden la existencia de un deber de facilitar información sobre los encargos de tratamiento a los interesados. Así, la Agencia Catalana del Protección de Datos (atendiendo a las circunstancias concurrentes en el tratamiento) apunta que puede resultar conveniente facilitar información sobre la existencia de encargados del tratamiento en aras de garantizar la aplicación del principio de transparencia. En este sentido, el propio GT29, en la Guía de Transparencia ("*Guidelines on transparency under Regulation 2016/679*") trata el tema de forma explícita y hace una precisión en el sentido de indicar que el término "destinatario" no ha de ser interpretado

exclusivamente como un tercero, sin que en esta categoría se ha de entender incluidos también a los encargados de tratamiento:

*"The term "*recipient*" is defined in Article 4.9 such that a recipient does not have to be a third party. Therefore, data controllers, joint controllers and processors to whom data is transferred or disclosed are covered by the term "recipient" and information on such recipients should be provided in addition to information on third party recipients".*

Esta interpretación ampliaría significativamente el concepto de destinatario, incluyendo a los encargados de tratamiento. En este inciso, de hecho, se apunta a la idea de incluir dentro de la categoría de destinatarios de datos personales a los responsables, encargados y corresponsables, lo que, interpretado en unión del artículo 13.1.e RGPD haría obligatorio informar sobre los encargados de tratamiento a los interesados, cuando hasta ahora no habría existido tal obligación de informar al interesado. Respecto de los responsables y corresponsables, nada que objetar, estaríamos ante una comunicación de datos puesto que en ambos casos los datos se van a tratar para una finalidad distinta (conexa o no) que tendrá otros responsables y por lo tanto son terceros a todos los efectos y hay que informar al interesado. Pero esto mismo no se puede predicar del encargo de tratamiento que pertenece a la esfera interna del tratamiento inicial realizado por el responsable.

Además, desde un punto de vista práctico, informar al interesado acerca de los encargados del tratamiento que pueden tener acceso a sus datos puede ser harto complicado además de muy inquietante y de escasa utilidad, para el interesado. Los encargados de tratamiento varían en el tiempo y en realidad su responsabilidad frente al interesado está intermediada por el responsable, que será quien deba responder en un primer término frente al interesado en caso de incumplimiento. Facilitar el detalle de todos los encargos de tratamiento más allá de constituir una tarea ímproba, pude generar más desconcierto que tranquilidad en el interesado. Al fin y al cabo, la información relevante para el interesado está en: quién es el responsable del tratamiento que ha de responder ante una eventual reclamación del interesado, qué datos se tratan, para qué y por cuánto tiempo. El resto de las consideraciones, se pueden dilucidar a través de una garantía de cumplimiento que puede y debe ofrecer el responsable, con independencia de quien sea el encargado. Por otra parte, obligar a informar sobre los encargados de tratamiento puede tener implicaciones en cuanto a los procesos de negocio y el *know how* de las compañías.

En cualquier caso, en la actualidad, mayoritariamente no se facilita información sobre los encargados de tratamiento bajo la interpretación de que no son destinatarios de la comunicación de datos.

Ahora bien, hay al menos dos dificultades relevantes para aplicar el esquema de encargo de tratamiento a los flujos de datos intragrupo.

La primera dificultad deriva de la propia naturaleza del supuesto de hecho planteado; es decir, de la existencia de una actuación conjunta del Grupo de Empresas frente a los terceros, al ofertar servicios, realizar procesos y desarrollar negocios de forma conjunta a todos los clientes del grupo, sin distinción en cuanto a la entidad filial con la que se entabló inicialmente la relación contractual. En el caso de lo que he dado en llamar Grupos de Empresa esto es un supuesto de hecho muy habitual. puesto que de cara al cliente y más allá de que se firme un contrato con una filial u otra, el cliente tiene la percepción de estar contratando con una única empresa, representada normalmente con el logotipo y nombre comercial de la matriz. Por poner un caso práctico, podemos pensar en una cadena hotelera en la que la matriz tiene todos los medios de producción, pero la titularidad de cada establecimiento hotelero pertenece a una filial del grupo. Todas funcionan bajo los procesos y con la capacidad productiva de la matriz, pero cuando el cliente se aloja en el establecimiento hotelero, quien le cede el uso de la habitación es la empresa propietaria del inmueble en cuestión, es con ella con la que de facto suscribe el contrato de alojamiento hotelero. Bajo el esquema del encargo del tratamiento se podría, en un primer momento, pretender regular todo lo referente a la gestión administrativa e incluso publicitaria implicada en la relación entre el cliente y la filial afectada, pero ¿qué sucede si la matriz decide implantar nuevos procesos que atañen a todos los huéspedes que se han alojado en todos los hoteles de su cadena? Por ejemplo, mediante una aplicación que permita la creación de una suerte de comunidad de usuarios de las instalaciones de los hoteles de la cadena o un programa de fidelización por puntos. La matriz no podría dirigirse a todos los clientes de las filiales para ofrecer este servicio, por una cuestión que se pone de manifiesto al ser planteada en este caso, pero que en realidad subyace en todo momento: la matriz no estaría realizando el tratamiento por cuenta del responsable; no hay un verdadero encargo de tratamiento.

El segundo problema es que, en efecto, en realidad tampoco cuando se configura la relación para la gestión administrativa entre la matriz y las filiales como un encargo de tratamiento estamos realmente ante esta figura. El encargado es la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento (de acuerdo con artículo 4 RGPD) y su característica distintiva es su dependencia de un responsable que se caracteriza "*por su capacidad de decisión en la concreción de los fines y los medios del tratmiento de los datos personales*", siendo esta una facultad indelegable en su integridad en el encargado (RODRÍGUEZ AYUSO, J. F.; 2019). En el ejemplo citado, quien está determinando la finalidad y medios del tratamiento no es la filial titular de la explotación hotelera, sino la matriz, la dueña de la marca comercial, titular de todos los procesos productivos, la que tiene la capacidad de control sobre todas sus filiales. Y, sin embargo, son las filiales del grupo quienes recaban los datos de los interesados, convirtiéndose en responsables del tratamiento por ese mismo hecho. Esto es así, porque la base de legitimación para el recabo de los datos de los clientes es la ejecución de la relación contractual que solo puede ser suscrita por el titular del negocio de explotación hotelera (las filiales en nuestro ejemplo). Para que se recabaran los datos directamente por la matriz se requeriría el consentimiento de los afectados, pero este es, por definición, libre y revocable. Dado que los datos de los interesados se necesitan en todo caso para la gestión de la relación contractual, ello nos obliga a replantear el esquema del encargo del tratamiento y buscar esquemas que permitan el uso de los datos de los interesados directamente por la matriz.

3.2. Corresponsabilidad

Este esquema parece estar pensado para uniones estables entre diferentes empresas, negocios de *joint venture* o simplemente la gestión de datos nacidos de una actividad regulada en acuerdos de colaboración entre empresas. Lo cierto es que no es fácil establecer su ámbito de aplicación teórico y práctico, porque el RGPD solo le dedica un artículo. Dicho artículo apunta en el sentido de posibilitar el establecimiento de una solidaridad en la responsabilidad ante el interesado, que podrá ser objeto de reparto en la esfera interna. Lo que está claro es que el esquema de corresponsabilidad parte de la premisa de que hay dos (o más) entidades actuando conjuntamente, que son responsables de un determinado tratamiento, siendo preciso delimitar frente a terceros las responsabilidades de cada uno.

3.2.1. Regulación

El RGPD aborda esta figura en el art. 26 RGPD refiriendo que, dos o más personas físicas o jurídicas son conjuntamente responsables del procesamiento, es decir, deciden conjuntamente sobre los fines y los medios de tratamiento. Al igual que en el caso del encargo de tratamiento, la existencia de un acuerdo escrito detallando los términos de la cooperación y delimitando las responsabilidades de cada parte es necesario, lo que requiere, entre otras cosas, una representación de las respectivas funciones y relaciones reales de las respectivas personas responsables frente al interesado. Aparte de este escueto artículo, la regulación legal no le dedica mucho más detalle y parece establecer un régimen de solidaridad frente al interesado en lo que respecta al ejercicio de sus derechos. Para comprender mejor esta figura, podemos acudir a la guía sobre los conceptos de responsable, encargado y corresponsable del Reglamento 2018/1725, aplicable al tratamiento de datos personales por parte de las instituciones europeas, publicada el 7 de noviembre de 2019, por el Supervisor de Protección de Datos de la Unión Europea (EDPS)

En esta guía se aporta luz sobre el concepto clave de la corresponsabilidad, la decisión conjunta sobre medios y fines. A este respecto, en la citada guía se indica que "*La noción de determinación conjunta debe entenderse como cualquier situación en la que cada responsable tiene la posibilidad / derecho de determinar los fines y elementos esenciales de los medios de una operación de tratamiento. Significa que, antes de celebrar un acuerdo específico con una o más partes, cada responsable es consciente del propósito general y (elementos esenciales de) los medios de tratamiento. En otras palabras, simplemente al celebrar dicho acuerdo, las partes comúnmente determinan (o convergen) el propósito y los elementos esenciales de los medios para llevar a cabo una operación de procesamiento: esto, en sí mismo, es suficiente para desencadenar una situación de control conjunto*" (traducción propia y énfasis añadido). Tales fines, que se determinarán mediante convergencia de voluntades, se deberán recoger por escrito de forma específica en un acuerdo, siendo este acuerdo el que determina la existencia de corresponsabilidad, por lo que todo tratamiento que exceda lo expresamente pactado será responsabilidad de la parte que lo lleve a cabo.

3.2.2. Aplicación práctica

No es fácil encontrar ejemplos de la aplicación práctica de este mecanismo previsto en el RGPD. Lo cierto es que, cuando las empresas desean llevar a cabo negocios conjuntos que

requieren establecer acuerdos de gestión comunes para llevar a cabo una empresa, se suele articular todo ello mediante en esquema elaborado a partir de una sociedad vehículo cuya finalidad es precisamente la de concentrar y aislar, en lo posible, todas las responsabilidades derivadas de la ejecución del negocio común a la vez que canalizar los beneficios hacia los socios en las proporciones convenidas previamente. En este planteamiento la corresponsabilidad no tiene cabida, puesto que habría una responsabilidad directa y única de la sociedad vehículo que, en caso de concretarse ya se derivaría por acuerdos entre partes a los accionistas.

En la práctica este esquema se puede ver en tratamientos de datos llevados a cabo por profesionales independientes prestando servicios a una empresa que a su vez ofrece sus servicios a un cliente y que, por la naturaleza de su profesión (o su interés en el tratamiento de los datos recabados), prefieran optar por un esquema de responsabilidad propia (vía cesión de datos o corresponsabilidad) en lugar de emplear la figura del encargo de tratamiento que limitaría el tratamiento permitido a lo estrictamente necesario para la prestación del servicio contratado. Por ejemplo, podríamos pensar en servicios médicos especializados vinculados a un centro hospitalario mediante convenio o acuerdo de prestación de servicios, supuesto que ha sido analizado por SCHÜTZE, B., KÄMMERER[1]..

En general, a priori, en el ámbito de los procesos aplicados que requieran un alto grado de especialización por procesos e intervención de múltiples entidades de forma coordinada, pueden darse casos de este tipo de acuerdos de corresponsabilidad.

Con vistas a futuro, es posible que esta figura pueda tener un mayor desarrollo próximo, afirmación que baso sobre el dictamen recientemente emitido por la autoridad de control alemana en materia de protección de datos, acerca de los requisitos y la información que debe facilitarse para el uso de *Google Analytics*. Este dictamen puede ser el precursor de un cambio de tendencia en el recurso a esta figura, en Alemania, al menos.

En opinión de la autoridad de control alemana, los operadores de sitios web que utilizan *Google Analytics* no tienen capacidad de decisión exclusiva sobre los medios y fines del

[1] *Vid*. más detalladamente, SCHÜTZE, B., KÄMMERER, M. Teleradiología legal: Implementación de requisitos de protección de datos. *Radiólogo* 59, págs. 637-642 (2019).

tratamiento, siendo en realidad Google quien tiene tal capacidad. En consecuencia, indica, esta no es una relación entre responsable y encargado en términos del Artículo 28 del RGPD, por lo que cualquier acuerdo de procesamiento que pueda haberse celebrado sería nulo. Además, señala que el tratamiento de datos que tiene lugar cuando se usa *Google Analytics* (es decir, el tratamiento y la transmisión de datos desde el sitio web del usuario al servidor de Google, el tratamiento en los servidores de Google para propósitos de *Google Analytics* y para otros fines) debe verse como un solo proceso, por lo que no existiría distinción entre el rol de responsable y encargado; esto es nuevo porque pone a Google y al usuario de *Google Analytics* en el mismo plano como controladores conjuntos en términos del Artículo 26 del GDPR. Habrá que estar a ver qué documento suscribe Google con los usuarios porque, y he aquí la clave del asunto, mientras que el RGPD regula profusamente el contenido y consecuencias del encargo de tratamiento, en materia de tratamiento conjunto, no lo hace.

En lo que al supuesto de hecho planteado en este estudio se refiere, la aplicación de esquemas de corresponsabilidad a Grupos de Empresa tiene aplicación limitada. Podría pensarse, en una primera aproximación que tuviera utilidad acudir a este esquema, regulando a nivel de grupo un acuerdo conjunto de utilización de datos, delimitando así responsabilidades en función de los tratamientos realizados por las distintas entidades que componen el grupo de empresas, pero eso no es lo que prevé la norma. Los tratamientos que se realizan en el seno de estos Grupos de Empresa los realizan cada una de las empresas y sobre bases de legitimación diferentes en cada caso; no se trata de tratamientos globales, no se trata de tratamientos cuya definición se haya consensuado conjuntamente por las diferentes empresas del grupo. Se trata de tratamientos diferenciados de cada entidad del grupo (con un paralelismo claro entre ellas) y cuyas notas principales son determinadas por la matriz del grupo en exclusiva.

Siendo el órgano decisor, en última instancia, el órgano de administración de la matriz del grupo, articular una corresponsabilidad puede resultar contraproducente:

(i) Por un lado, la información a facilitar a los interesados se complica notablemente. En aras del principio teórico de transparencia habrá que informar de todos los corresponsables y su participación en el tratamiento, lo cual, no siendo siempre de fácil comprensión, puede ir en detrimento de la transparencia real en el tratamiento de datos personales; y,

(ii) a nivel de reparto de responsabilidades interno, no parece que tenga mucho sentido tampoco, pudiendo incluso suponer un riesgo agravado en caso de incumplimiento o daño, por aparecer en el horizonte más de un responsable del tratamiento al que dirigir una reclamación, sin que además quede claro en la norma cómo funciona el régimen de solidaridad o responsabilidad individual que existe en relación con la figura del corresponsable. La clave, en último término, está en determinar si los acuerdos de corresponsabilidad son oponibles frente a terceros delimitando responsabilidades o si operan solo en la esfera interna entre los diferentes responsables. La norma no lo específica. A este respecto, en el Dictamen 1/2010 del GT29 se dice: "*que 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" y añade que "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*".

En la práctica, este deslinde de responsabilidades es lo que debe quedar establecido en el contrato de que las partes deberán suscribir para regular su actividad de tratamiento conjunto, pero frente a un tercero, la solidaridad es inevitable, o acaso se le va a exigir al interesado que conozca los detalles de este acuerdo y en caso de litigio deba dirigirse necesariamente a todos los corresponsables, exigiéndose el litisconsorcio pasivo necesario, lo cual no deja de suponer una carga adicional para el interesado en la defensa de sus derechos. Aun es escasa la jurisprudencia en esta materia, por lo que no existe demasiada claridad meridiana sobre el reparto de responsabilidades en el caso de tratamiento conjunto. Mientras esto sea así, será un planteamiento cuya aplicación tenderá a rehuirse, en lo posible.

3.3. Cesión de datos

Esta forma de comunicación de datos es la que procede establecer en todos los casos que no encajan en el esquema de encargo de tratamiento. Dentro de un mismo grupo empresarial es de pensar que pueda existir una multiplicidad de cesiones, por razón de los negocios que se lleven cabo a través de diferentes filiales en un mismo conglomerado empresarial. Pero lo que determina que estemos ante una cesión es que haya dos responsables de dos tratamientos diferenciados sobre unos mismos datos iniciales. Este esquema, es el más adaptativo para la regulación de los flujos de datos entre compañías del mismo grupo de empresas, pero también es más gravosa su gestión.

3.3.1. Regulación

Interesa en este caso analizar la regulación aplicable desde una perspectiva evolutiva desde la LO 15/1999 de 13 diciembre de 1999 de Protección de Datos Personales (en adelante "LOPD"), hasta el RGPD y la LOPDGDD.

La LOPD sentaba como requisito general para la cesión de datos el consentimiento (art. 11 LOPD), y a partir de esta regla general establecía determinadas excepciones (cesiones autorizadas por ley, cesiones de datos obtenibles de fuentes accesibles al público, cesiones basadas en una relación jurídica aceptada que necesariamente implique la cesión —lo que no deja de ser un consentimiento—y determinadas cesiones a organismos públicos o Administraciones Públicas, o cesiones para solucionar urgencias de salud en los términos establecidos en la legislación aplicable). También se contemplaba la obligación de informar al interesado en el momento en que efectivamente tuviera lugar la cesión de sus datos; bastando con informar sobre la finalidad del nuevo tratamiento, los datos cedidos y la identificación (razón y domicilio social) del cesionario (art. 27 LOPD).

Se hizo muy extendida en la práctica empresarial, al amparo de esta legislación, la idea de que la cesión siempre requería del consentimiento del afectado y, si bien esta afirmación no es exacta, sí que se aproxima bastante a la realidad. Tan extendida resulta que no era infrecuente (y aun hoy sigue siéndolo) que el consentimiento se trate como base de legitimación preferente y cuasi exclusiva de la cesión de datos. Y, sin embargo, el enfoque que se da a la cuestión con el RGPD es otra.

El RGPD no dedica ningún apartado específico a la cesión de datos. Lo que hace es regular con intensidad la información que se ha de suministrar al interesado con carácter previo para el tratamiento de sus datos personales, tanto si son recabados directamente del interesado como si no (Art. 13 y 14 RGPD). Ello nos lleva a concluir que se asume de algún modo que la cesión de datos va a ser el paradigma principal y la norma regula cómo proceder en tales casos a los efectos de informar al interesado. A este respecto, el GT29, en la ya citada guía de transparencia ("Guidelines on transparency under Regulation 2016/679") alude a la posibilidad de realizar cesiones de datos sin nominar expresamente al cesionario, sino de forma genérica, por referencia a la industria, sector o subsector añadiendo su ubicación:

"In accordance with the principle of fairness, controllers must provide information on the recipients that is most meaningful for data subjects. In practice, this will generally be the named recipients, so that data subjects know exactly who has their personal data. If controllers opt to provide the categories of recipients, the information should be as specific as possible by indicating the type of recipient (i.e. by reference to the activities it carries out), the industry, sector and sub-sector and the location of the recipients".

De algún modo parece que se estuviera compensando la exigencia, acaso excesiva, de identificar a los encargados de tratamiento (ver apartado 2.2.1. anterior), con una cierta permisividad en la identificación de forma genérica de los cesionarios. Sin embargo, en aras de la trasparencia informativa, no deberíamos olvidar que el responsable del tratamiento será responsable del tratamiento que él haga, pero no así de los que hagan los cesionarios y por lo tanto la determinación de estos debería ser clara y concisa de modo que se permita el ejercicio de la autodeterminación informativa.

Aun se escuchan voces que defienden la necesidad de contar con el consentimiento para llevar a cabo una cesión de datos, pero nada más lejos de la realidad. Siguiendo la estela de los supuestos que permitían excepcionar la necesidad de contar con el consentimiento bajo la derogada LOPD, ahora hay que aplicar los principios generales de licitud del tratamiento. Dicho de otro modo, se normaliza el régimen de cesión de datos que puede ampararse en cualquiera de las bases de legitimación, como cualquier otro tratamiento; ello incluiría el interés legítimo con todos los caveat que el uso de esta base de legitimación debe conllevar. Dado el cambio relevante que supone amparar la cesión de datos en el interés legítimo

respecto de la normativa anterior, conviene detenernos en el análisis de este concepto. No obstante, y por exponer toda la situación normativa anterior al RGPD, hay que puntualizar la que el artículo 7f) de la Directiva 46/95/CE sí contemplaba el interés legítimo como base legitimadora de una cesión de datos siempre que no prevaleciera el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la Directiva. Ahora bien, la LOPD no recogió este supuesto en su artículo 11.

El GT 29 en la Opinión 06/2014 (844/14/EN WP 217) precisa qué se ha de entender por interés legítimo. En cuanto al concepto de interés, se trataría del beneficio que puede obtener el responsable que deberá: (i) estar expresamente manifestado; (ii) ser claro; (iii) real; (iv) presente (no basta con una mera expectativa futura); y, (v) guardar relación con la misión propósito o finalidad perseguida por el responsable del tratamiento. El GT29 apunta además que el interés bien puede ser de un tercero (incluida la sociedad en su conjunto —la Directiva 46/95/CE, y ahora el RGPD, admiten el interés legítimo de terceros como base de legitimación) en cuyo caso podría estar estrechamente vinculado a un interés colectivo, de la sociedad. Por poner un ejemplo de actualidad, la publicación de memorias de prevención de blanqueo de capitales o de responsabilidad social empresarial (a nivel de grupo o de la matriz de un grupo empresarial) que buscan poner de manifiesto los esfuerzos (y resultados) empresariales en la lucha contra el fraude y la corrupción proporcionan datos agradados que parten del tratamiento de datos de origen individualizados cuyo tratamiento respondería a este interés (todo ello sin perjuicio de la necesaria adopción de medidas de salvaguarda adecuadas). A este respecto el artículo 6.1.f RGPD, contempla como causa legitimadora para el tratamiento de datos el interés legítimo. En cuanto al carácter legítimo del interés, en principio entiendo que se ha de equiparar con un carácter no antijuridico del mismo (el GT 29 ofrece la una lista abierta de supuestos en la citada opinión que no tiene mayor interés reproducir en este punto) y, en todo caso, debe ponderarse siempre con su posible impacto en los derechos y libertades fundamentales de los afectados; debiendo quedar justificado la necesidad idoneidad y proporcionalidad del tratamiento que se pretende a los efectos e ponderar adecuadamente si esta base de legitimación es suficiente o no. A efectos de efectuar la ponderación exigida deberá plantearse si, atendiendo a las circunstancias concretas concurrentes en cada situación analizada, el interés del tercero (cesionario) en acceder a los datos que sean objeto de comunicación o cesión debe prevalecer sobre el

derecho a la protección de datos de los interesados, personas físicas titulares de los datos que sean objeto de tal comunicación o cesión. Y en este análisis es esencial introducir la valoración de la finalidad del tratamiento, o de la cesión en este caso.

La determinación de la finalidad de la comunicación es esencial para validar la existencia o no de esta base de legitimación. Así, el artículo 5.1.b) RGPD sienta el principio de limitación de la finalidad, indicando que "*los datos personales serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales*". Pero acaso más esclarecedor que los artículos 5 y 6 del RGPD lo es el considerando 47 que establece que "*El interés legítimo de un responsable del tratamiento, incluso el de un responsable al que se puedan comunicar datos personales, o de un tercero, puede constituir una base jurídica para el tratamiento, siempre que no prevalezcan los intereses o los derechos y libertades del interesado, teniendo en cuenta las expectativas razonables de los interesados basadas en su relación con el responsable*"; y añade que "*la existencia de un interés legítimo requeriría una evaluación meticulosa, inclusive si un interesado puede prever de forma razonable, en el momento y en el contexto de la recogida de datos personales, que pueda producirse el tratamiento con tal fin*" (énfasis añadido). Esta idea de la expectativa razonable no se desarrolla posteriormente en el articulado, pero en el RGPD se establece como punto de partida necesario que ha de tenerse en cuenta y es indudable que tiene vinculación directa con la finalidad ulterior a la que el cesionario destine los datos. Dicho de otro modo, el interés legítimo debe serlo del cedente, pero debe responder a una expectativa racional y razonable en la mente del interesado titular de los datos, de que eventualmente pueda producirse tal cesión. Así pues, para el análisis de la posibilidad de la comunicación será necesario determinar si la finalidad para los que se recogieron los datos es distinta de la finalidad que se pretende conseguir con la cesión. Dados todos los condicionantes, no es la base jurídica más sólida ni más permisiva para regular la cesión de datos. De hecho, en alguno de sus aspectos, como la necesidad de existencia de una vinculación en la finalidad se asemeja mucho a la base jurídica consistente en la necesidad de ejecución de un contrato.

Centrándonos en esta última base de legitimación, la ejecución de una relación contractual, esta sería la base aplicable a la cesión de datos en la medida en la que para la ejecución de los distintos acuerdos alcanzados en el contrato suscrito sea necesario que intervengan distintas compañías. Es decir, que los servicios son prestados directamente al cliente por distintas compañías. Por poner un ejemplo, al contratar un viaje organizado, se necesitará la comunicación de los datos para la ejecución de todas las prestaciones contratadas, en las que intervienen distintas compañías que trataran los datos para sus correspondientes fines independientes, pero ligados a la ejecución del propio viaje contratado (alojamiento, *tee tim*e de golf, servicio de restaurante en pensión completa, excursiones prefijadas, transportes en el entorno, etc.).

3.3.2. Aplicación práctica

Es evidente que dentro de cualquier grupo de empresa se dan flujos de datos en los que el responsable del tratamiento comunica los datos a otras de las empresas del grupo para una finalidad distinta, conexa o no con la inicial. En estos casos no hay vuelta de hoja, se trataría de cesiones de datos en toda regla y difícilmente cabe interpretar algo diferente. Evidentemente, estas cesiones, además de cumplir con los requisitos de información del artículo 14 del RGPD, deben disponer de una base de legitimación que bien podría ser la necesidad para la ejecución de un contrato, el interés legítimo, tal y como antes se ha indicado, o el consentimiento. Y será en función de la finalidad, del carácter necesario o no de la cesión, de si hay un equilibrio adecuado entre los derechos de cedente, cesionario e interesado, que se deberá determinar la base legitimadora de la cesión y su amplitud o contenido; pues no nos olvidemos que, en todo caso, la cesión, igual que el recabo inicial de datos debe prestar el principio de limitación de la finalidad.

El problema de basar la cesión en el consentimiento radica en que éste siempre, por naturaleza, es revocable; basarse en el carácter necesario para la ejecución de un contrato sólo cubre determinado tipo de cesiones que muchas veces puedan articularse como encargos de tratamiento. Será frecuente que se dé este tipo de cesiones en grupos de empresas que ofrezcan paquetes de servicios a sus clientes o entre empresas con acuerdos comerciales para facilitar un servicio conjunto. Fuera de estos contextos, son supuesto que no son tan sencillos de aplicar y lejos de aportar claridad al interesado y certeza en cuanto a la realización del tratamiento de forma legítima y continuada por el responsable, suscitan

suspicacia y no dan suficiente certidumbre en cuanto a la posibilidad de mantener el tratamiento en el tiempo.

La posibilidad de amparar la cesión en el interés legítimo habilita un nuevo campo de aplicación para esta figura que puede encontrar acomodo razonable para regular los flujos de datos dentro de grupos de empresa que realizan actividades conexas o idénticas entre sí y la matriz. No es la base más sólida en tanto que requiere articular cuidadosamente el juicio de ponderación y la conexión finalista que justifique la existencia de una expectativa razonable de cesión en el interesado (que además, para dar debida satisfacción al principio de responsabilidad proactiva, debería documentarse por escrito) pero amplía el espectro de posibilidades para articular una cesión sin tener que acudir al consentimiento expreso que, como ya se ha dicho plantea un problema práctico relevante, que complicaría seriamente la gestión de los datos hasta el punto de poder llegar a convertir en inviable un negocio; debido a la naturaleza siempre revocable del consentimiento.

Tradicionalmente, el asesoramiento profesional en materia de protección de datos, por el motivo que fuere, acaso incluso por falta de una verdadera especialización en la materia, pasaba necesariamente por la exigencia de prácticamente toda cesión de datos se habría de basar en un consentimiento previo. Y en la práctica el consentimiento se recababa dentro de clausulados que a menudo son más largos que el propio contrato al que hacen referencia; y ello con independencia de que la cesión fuera o no necesaria para la ejecución del contrato.

En definitiva, la normalización de la posibilidad de basar la cesión de datos en cualquiera de las bases de legitimación previstas en el artículo 6 RGPD, incluyendo el interés legítimo abre una puerta a la regularización de las cesiones de datos entre empresas de la que normalmente se ha tendido a huir en la medida de lo posible en el ámbito empresarial, por cuanto el consentimiento era la pieza clave sobre la que se fundaban habitualmente. Poder basarlas en las restantes bases de legitimación del RGPD abre la puerta a un escenario de mayor claridad, y una mayor coherencia en la aplicación práctica de la regulación, lo que, en materia de protección de datos, siempre ha sido bastante retador.

Aun así, la normativa exige siempre que en el caso de recabarse los datos de un tercero distinto del propio titular de los datos se le informe al interesado de la existencia de este nuevo tratamiento resultante de la cesión, con indicación de la proveniencia de los datos obtenidos (art. 14 RGPD). Lo cierto es que esta obligación no siempre se cumple, al menos

no de forma transparente y clara en buena parte de los casos.; en general las empresas no desean saturar al cliente con mensajes que ocupan espacio y consumen la atención del cliente sin dar un rédito comercial a cambio. En el caso concreto de las cesiones dentro de un Grupo Empresarial en muchas ocasiones éste se presenta ante terceros como una única entidad, representada a través de un único nombre comercial; por lo que los terceros desconocen realmente la identidad del responsable del tratamiento y asumen de algún modo que contratan con una única entidad que responderá unitariamente.

Volviendo al ejemplo anterior, relativo a la contratación de un viaje con diferentes prestaciones de terceros asociadas al mismo, pongamos ahora por caso que todas esas prestaciones (alojamiento, *tee time* de golf, servicio de restaurante en pensión completa, excursiones prefijadas, transportes en el entorno, etc.) son realizadas por empresas del mismo grupo empresarial que frente al cliente se identifican bajo una única denominación comercial y en realidad el cliente contrata únicamente con una de dichas empresas que luego subcontrata o transfiere precios y costes con las demás empresas del grupo. En estos casos, a pesar de que para el interesado solo existe un responsable, en realidad se le informa de la diseminación de sus datos a través de hasta cinco empresas (en el ejemplo indicado); y qué sentido tiene esta dispersión; ante quién debe ejercitar sus derechos en caso de incumplimiento; de conformidad con el artículo 14 RGPD cuando se empleen los datos del cliente las cesionarias deberían notificárselo al interesado; y el interesado, cuando menos, se extrañará al recibir tales comunicaciones, pues lo más probable es que no sepa de qué se trata y además le generará cierta sensación de pérdida de control o de abuso por parte de la empresa comunicante.. Cabe pues preguntarse si no sería más sencillo, en aras de la transparencia informativa y de la simplicidad operativa, aglutinar todos los tratamientos intragrupo en uno solo de cara al interesado cuando la naturaleza de los procesos ejecutados y la forma de presentarse la entidad al mercado lo permitan.

Y trasladando el argumento un poco más allá, en lo que he denominado Grupos de Empresa, donde las filiales son cascarones vacíos en los que únicamente hay un activo productivo y todo lo demás, incluida la actividad comercial, la imagen de marca y el nombre comercial son solo uno frente al cliente; y generalmente responden a los datos de la matriz, pierde todo sentido. La matriz del grupo es la entidad con la que el cliente —el interesado desde la perspectiva de protección de datos— realmente tiene interés en contratar; la existencia a de

la matriz al frente del Grupo de Empresa constituye la razón final última que mueve la voluntad del cliente para suscribir el contrato de que se trate; es la matriz con quien el cliente tiene la noción de estar contratando, aunque la formalización del acuerdo se materialice con una filial. Tratar de explicar a un cliente el régimen de cesiones para el tratamiento de los datos necesarios para la prestación del servicio solicitado parece un auténtico despropósito que más que facilitar el cumplimento de la norma lo complica y genera recelo en el interesado que, después de todo, en quien confía es en la entidad que se le ha representado durante todo el proceso comercial, y que, como digo, suele ser la matriz. Lo que quiere el cliente y es la clave de todo, es que, en último término, sea el grupo empresarial, con la matriz a la cabeza, quien asuma las responsabilidades asumidas en todo caso, por las filiales que instrumentalmente participen en la relación contractual de que se trate.

4. Hacia un nuevo planteamiento: ¿es posible la aplicación de la norma a nivel de grupo?

4.1. El porqué de un posible nuevo planteamiento

Hasta aquí, se ha analizado como se podrían articular los flujos de datos entre empresas del mismo grupo, pero vale la pena plantearse si no habría una forma más garantista y eficiente que la de aplicar de forma independiente a cada empresa del Grupos de Empresa la normativa vigente. Se trata de un ejercicio teórico especulativo cuyo único apoyo reside en la interpretación del Tribunal Supremo que, sin entrar a analizar el hecho de que no existe una base positiva para hacer esta interpretación, sí indica que no cabe hacer una aplicación de la normativa de protección de datos a nivel de grupo, en perjuicio de tercero. Esto deja abierta la especulación a teorizar sobre qué sucedería si existe no se produjera tal perjuicio. Para este propósito, el punto de partida ha de ser el análisis de los principales impactos que puede tener en la práctica la obligación de aplicar la normativa de forma independiente en cada una de las entidades de un Grupo de Empresas tomando en cuenta tanto la perspectiva del interesado como del responsable del tratamiento.

No es tarea primordial del legislador atender a todos los detalles que pueden derivarse de la aplicación práctica de las normas que se dictan. Más bien es al revés, las normas se dictan para moldear y modular la conducta de los agentes sociales en el sentido que aquellas prescriben. El resultado de la regulación de aspectos complejos como la protección de datos en un contexto de desarrollo creciente de la tecnología y la digitalización da como resultado una norma que puede resultar compleja y que se olvida de la realidad de multitud de empresas de tamaño medio a las que les cuesta mucho llegar a cumplir el estándar exigido. Este fenómeno ha sido especialmente llamativo en el contexto de la promulgación y entrada en vigor del RGPD.

En lo que a la cuestión objeto de este estudio se refiere, el cumplimiento, de forma independiente, de todos los requisitos informativos de los artículos 13 y 14 RGPD por cada una de las entidades pertenecientes a un Grupo de Empresas cuando todas ellas llevan a cabo o participan en la realización de un mismo tratamiento da como resultado la necesidad de realizar múltiples comunicaciones a los interesados y, por consiguiente, la necesidad de

diseñar multitud de procesos internos para dejar evidencia de la existencia de todos los documentos informativos con la precisión y claridad exigibles. Esto que parece una tarea simple y sencilla puede ser bastante laborioso, cuando no complejo, en función de la base de legitimación de cada tratamiento.

Si estamos ante tratamientos cuya base de legitimación es el consentimiento será algo relativamente sencillo, puesto que con explicitar todos los tratamientos afectados y sus respectivos responsables se podrá dar cumplimiento a la normativa aplicable, sin necesidad de articular ningún tipo de cesión de datos, ni comunicaciones posteriores resultantes de la realización de las mismas.

Ahora bien, si el tratamiento nace sobre la base de un interés precontractual o de la ejecución de un contrato suscrito con el interesado, el responsable será necesariamente la empresa concreta que haya suscrito ese contrato y ninguna otra del grupo de empresas. Así pues, en esos contratos siempre habrá que prever la cesión o el encargo de tratamiento a las restantes empresas que, por razón de los procesos que realizan, puedan acceder, o tratar los datos del interesado. Exponer esta información puede no ser complejo, pero desde luego tampoco va a ser claro o transparente para el interesado, que normalmente desconocerá la estructura del grupo. Además, en el momento de recabarse dichos datos la entidad destinataria de los datos debería posteriormente informar de la obtención, tratamiento y proveniencia de los datos recibidos. En la práctica es poco frecuente que esto suceda y, en la práctica, tiende a minimizarse esta información que se facilita deliberadamente de modo en que al interesado le pase desapercibido En relación con esta afirmación cabe traer a colación varias sentencias relativas a la actividad de comercialización y distribución de gas en las que, como consecuencia de la segregación del sector por actividades consecutivas pero diferenciadas, tiene lugar la cesión de los contratos (y por tanto de los datos aparejados a éstos). De la noche a la mañana el interesado pasó a tratar con al menos dos empresas (comercialización y distribución) cuando antes solo trataba con una.

Así, en la sentencia de la Audiencia Nacional 425/2009 de 24 junio de 2010 se expone claramente el problema de fondo que subyace a estas cesiones intragrupo al indicar que "*La circunstancia expuesta, tratamiento inicial por la distribuidora con apariencia formal de corrección de la contratación inicial, ha generado una cadena de funcionamiento en las empresas del grupo Gas Natural, en gran medida debido a la división de las actividades*

impuesta por la legislación de hidrocarburos y su exclusiva especialización". Conviene tener en cuenta que este asunto se recurrían sendas sanciones de 100.000 euros cada una por haberse producido una transmisión de datos personales de los clientes tanto de la filial de distribución como de la filial de comercialización, a la filial informática (necesaria para la facturación). En este asunto, las filiales de Gas Natural sancionadas por haber comunicado datos a la filial informática que gestionaba la base de clientes no acreditaron disponer de un contrato que habilitara la comunicación de datos, siendo esto la falta de un contrato, que no de un proceso formal de cesión, lo que, en última instancia supuso la ratificación de las sanciones recurridas.

Llama la atención de esta sentencia que no se entra a dilucidar qué clase de contrato habría de haberse firmado: encargo, cesión, acuerdo de corresponsabilidad.... dando a entender que cualquiera hubiera bastado. Se convierte así el contrato en un requisito formal imperioso en materia de protección de datos; mientras que, en el tráfico civil, el pacto verbal es válido y el documento constituye un medio de prueba.

? Parece baladí, pero documentar todas las relaciones intragrupo y comunicar al interesado todas las comunicaciones resultantes de los flujos internos exige una dotación no desdeñable de recursos para empresas de menor entidad; y en último término, puede resultar contraproducente, en tanto no aporte valor real y consuma tiempo y atención del interesado. . Así las cosas, en tanto todas las empresas de un Grupo de Empresas son consideradas sujetos obligados de la normativa de forma autónoma, todas aquellas entidades del grupo que reúnan los requisitos previstos en la normativa deberán designar DPO y llevar su propio Registro de Actividades de Tratamiento; independientemente del hecho de que el DPO será normalmente único o supeditado a la dirección del DPO de la matriz y que el Registro de Actividades de Tratamiento será prácticamente un calco (o una versión espejo) del de la matriz. Eso sí, un calco o versión espejo que hay que mantener y actualizar de forma permanente, por lo que, si el grupo tiene multitud de sociedades, el trabajo se multiplica, mientras que el valor añadido no es correlativo.

Se podría argumentar que la existencia de estos procedimientos internos independientes es una garantía para el interesado, por cuanto elaborarlos exige un esfuerzo de organización y control de los flujos de datos que le afectan en el contexto de cada entidad del grupo. Si esto es así, en sentido contrario, cuando las empresas del grupo sean tan pequeñas que no

reúnan los requisitos que hacen exigibles la formalización de un registro de actividades del tratamiento o la designación de un DPO, ¿acaso está más desprotegido el interesado? Pienso que no. Además, el criterio sentado por el Tribunal Supremo al sostener que el cumplimiento de la normativa debe ser independiente y aplicable a cada entidad autónomamente, aplicado al ámbito de la responsabilidad, conduce a concluir que la responsabilidad también será independiente y en función del capital social de cada empresa del grupo esto sí puede redundar en una menor protección.

4.2. Tendencias en la aplicación del RGPD y su impacto en la mediana empresa

Los progresos que se van dando en materia de derechos subjetivos en los últimos cincuenta años en España no son pocos y se han ido construyendo unos sobre otros de forma progresiva, pero el reconocimiento de un derecho por sí mismo no basta para asegurar su efectiva realización. Siguiendo a LUCAS MURILLO DE LA CUEVA (2007, pág. 22), esta afirmación, que se puede predicar de cualquier derecho subjetivo, es significativa en relación con la protección de datos, entre otras cosas porque es vicaria de la transformación de la sociedad a un entorno cada vez más tecnológico y digital, actualmente en pleno desarrollo a un ritmo vertiginoso y cada vez más acelerado. El citado autor destaca que las leyes han trazado un marco general de protección de datos que proporciona normas abiertas susceptibles de ser aplicadas a una multiplicidad de supuestos de hecho, pero que por eso mismo encuentra difícil acomodo para regular algunos ámbitos especialmente complejos de la sociedad; cita, entre otros, los tratamientos de datos de carácter personal de los juzgados y tribunales, los tratamientos de currículos en el ámbito educativo y de los pacientes en el ámbito de la salud, apenas regulados. Debe tenerse en cuenta que la publicación de este artículo data de 2007; antes de la llegada del RGPD, y de determinadas normas especiales. Lo cierto es que la afirmación puede considerarse válida aún hoy día, si bien actualizada al hecho de que ya se han ido promulgando leyes especiales para cubrir aspectos concretos no previstos en la norma general (en concreto en el ámbito sanitario, en el de la administración electrónica, o en el educativo, por mencionar alguno de los destacados por el citado autor). No obstante, la norma sigue sin dar un adecuado acomodo a las empresas pequeñas y medianas que apenas desarrollan procesos tecnológicos complejos y que se ven envueltas en el cumplimiento de una normativa extensa y compleja, pensada para un mundo en desarrollo tecnológico muy potente que a ellas les afecta, pero llevan un ritmo inferior, que

debe acompasarse con su modelo de crecimiento empresarial. En toda empresa de tamaño medio en crecimiento llega un punto en que debe dar un salto a la categoría de gran empresa y ello comporta la necesidad de invertir en recursos de estructura que suponen un incremento de su coste fijo estructural. Esto es así en todas las áreas de gestión empresarial y muchas veces esta transición no es tenida en cuenta por el regulador, que no hace distingos entre grandes y medianas empresas. El riesgo de no introducir esta estructura de cumplimiento normativo comporta un riesgo cierto elevado, especialmente en esta materia, dada la cuantía de las sanciones y la sensibilidad social existente hoy día con la protección de datos. Es un riesgo que, a veces, no se compadece bien con el tipo de tratamientos que se llevan a cabo en dichas entidades y que es necesario abordar de una manera que no sea especialmente gravosa para la empresa para mitigar el riesgo sin menoscabo de los derechos y garantías de los interesados. Este debate de la efectividad de la norma y su aplicabilidad real es necesario no dejarlo de lado.

En este sentido tiene interés la lectura de Informe de Evaluación sobre la aplicación del RGPD, emitido por la Comisión el momento en que se cumplen dos años desde la entrada en vigor del RGPD, donde, entre otras cuestiones, reconoce abiertamente las dificultades que encuentran las pequeñas y medianas empresas a la hora de aplicar el RGPD (*Commission Staff Working Document accompanying the documment Communication from the Commission to the European Parliament and the Council; 2020*).

Para contextualizar el análisis del informe es necesario comprender y valorar la especial circunstancia que rodea el tejido empresarial español. España es un país donde el 99% del tejido productivo está formado por autónomos y pymes (Ministerio de Trabajo, 2019); es decir, entidades de menos de 250 empleados, y un volumen de negocio menor o igual a 50 millones de euros o un balance que no supere los 43 millones de euros[2]. Esta definición no es incompatible con la de grupo de empresa; es más, es en empresas medianas donde con frecuencia nacen pequeños grupos de empresas con la vocación de expandir el modelo productivo limitando la responsabilidad aparejada en cada nuevo negocio; y a este respecto,

[2] *Vid*. Definición de mediana empresa contenida en el Anexo I del Reglamento (UE) nº 651/2014 de la Comisión, de 17 de junio de 2014, por el que se declaran determinadas categorías de ayudas compatibles con el mercado interior en aplicación de los artículos 107 y 108 del Tratado

hay que tener en cuenta que existirá grupo de empresa cuando exista unidad de decisión (art. 42 CCo), lo que puede producirse por medios societarios (por mor de una relación de dominio, que implica la existencia de una sociedad dominante, socio de la filial de forma directa o indirecta) o extrasocietarios (por la existencia de una dirección única, por ejemplo, mediante concomitancia de consejeros o altos directivos).

A nadie se le escapa que la normativa del RGPD es bastante exigente en cuanto a obligaciones se refiere para los sujetos obligados, obligaciones que pueden ser muy gravosas para esas pequeñas y medianas empresas. La Comisión, de hecho, no es ajena a esta afirmación y, en su informe, expone la existencia de una percepción general de los sujetos obligados —y reconocida por el Parlamento Europeo, el Consejo y las autoridades de protección de datos— consistente en que la aplicación del RGPD es especialmente desafiante para pequeñas y medianas empresas. A este respecto, la Comisión apunta a la consolidación del enfoque metodológico basado en el riesgo como el camino óptimo para encontrar una solución que permita dar cumplimiento a la norma y garantizar los derechos de los interesados sin sobrecargar innecesariamente a los sujetos obligados. La Comisión incide en que "*el tamaño no es en sí mismo una indicación de los riesgos que el procesamiento de datos personales cuyo cumplimiento deficiente puede conllevar para individuos*" (traducción propia del inglés). En efecto, el enfoque basado en el riesgo permite combinar flexibilidad con protección efectiva; y esto se podría predicar tanto de las pymes como de las grandes empresas.

Del análisis de la Comisión, cabe concluir que es necesario encontrar la fórmula que permita flexibilizar la aplicación de la norma para dar solución y cobertura a todos los riesgos que existan en materia de protección de datos, pero sin sobrecargar o exigir una cantidad de recursos desproporcionada cuando dichos tratamientos apenas conlleven riesgo. Si una empresa pequeña desarrolla procesos que, por su naturaleza, contexto, intensidad de tratamiento o cualidades innovadoras de la tecnología empleada, implican un riesgo elevado para los derechos y libertades individuales, deberán velar por el cumplimiento detallado y exhaustivo de la normativa aplicable, desarrollando proceso internos y medidas de seguridad adicionales si es preciso; pero paralelamente, cuando se trate de procesos auxiliares administrativos, de gestión o de servicios de escasa intensidad tecnológica o que impliquen un limitado tratamiento de datos personales con escaso riesgo asociado para los

derechos y libertades individuales, podría teóricamente admitirse una flexibilización en la intensidad de aplicación de la norma; modulada eso sí, por el hecho de que las grandes empresas sí suelen tener una estructura mayor, que sería capaz de asumir las obligaciones que impone la normativa de protección de datos.

En cuanto a las áreas que la Comisión ha identificado específicamente como más engorrosas (en palabras de la Comisión) en cuanto al cumplimiento de la normativa para las pymes, es la llevanza del registro de las actividades de tratmiento y consideran que la exención prevista en el artículo 30.5 RGPD es de limitada. A este respecto la Comisión matiza que "*los esfuerzos relacionados para cumplir con esa obligación no deben ser sobreestimados. Cuando el negocio principal de las PYME no implica el tratamiento de datos personales, dichos registros pueden ser simples y no onerosos*" y añado que "*en cualquier caso, todos los que procesan datos personales deben tener una visión general de su procesamiento de datos como un requisito básico del principio de responsabilidad*" (*Commission Staff Working Document accompanying the documment Communication from the Commission to the European Parliament and the Council; 2020; pág. 26;* traducción propia del inglés).

Por último, a este respecto la Comisión propone tres tipos de herramientas para facilitar el cumplimiento de las empresas: (i) el uso de los códigos de conducta; (ii) el fomento de los mecanismos de certificación y (iii) el empleo de cláusulas contractuales estandarizadas. En la práctica, los códigos de conducta, si no disponen de margen para aplicar la norma de una forma flexibilizada, tienen más sentido en empresas de tamaño grande, con la finalidad de garantizar la aplicación uniforme de proceso internos, dando la publicidad necesaria hacia los grupos de interés; mientras que en empresas pequeñas esta función carece de tal relevancia pues normalmente su implementación implica costes desproporcionados (tal y como reconoce la propia comisión a renglón seguido en su Informe). Lo mismo se puede predicar de los mecanismos de certificación que, si bien son muy cómodos cuando ya se han implantado, no son nada sencillos (ni baratos) de obtener; de lo que sí se beneficia la pyme es de subcontratar procesos con entidades más grandes a la que debería exigir la certificación, pero esto también comporta un coste y no reduce significativamente la carga del cumplimiento de la norma. Lo que sí puede tener utilidad real es el uso de cláusulas contractuales estandarizadas; pues recurrir a ellas reduce el coste de su elaboración y

negociación. Ahora bien, esta solución, que puede ser muy útil a la hora regular cuestiones tales como el flujo de datos intragrupo, presenta, al menos, dos dificultades:

(i) Deben existir estas cláusulas. A día de hoy, hay cláusulas contractuales para la transferencia internacional de datos y de para la suscripción de encargos de tratamiento, pero ya hemos visto que no todos los flujos intragrupo responden a este esquema de encargo de tratamiento. El régimen de corresponsabilidad no goza de un modelo de contrato y es una figura escasamente desarrollada en la práctica, el RGPD apenas le dedica unas líneas e implica una regulación ad hoc en cada caso que hace complicado que se pueda estandarizar el clausulado completo.

(ii) Las cláusulas contractuales tipo tienden a ser tan exhaustivas como la norma; por lo que darles cumplimiento es igualmente complicado. El resultado puede ser suscribir documentos que finalmente sean imposibles de cumplir.

En definitiva, estos mecanismos que ofrece la Comisión no son suficientes por lo que respecta a facilitar la regulación del cumplimiento a nivel interno en relación con los flujos de datos que se pueden intercambiar en el seno de un grupo de empresas.

4.3. *Habeas Data* como garantía de la autodeterminación informativa.

Si la perspectiva de la empresa en materia de protección de datos incide en el riesgo del procesamiento y las responsabilidades aparejadas, como se ha ido exponiendo, desde el punto de vista del interesado la clave reside en la garantía de sus derechos frente a la materialización de tal riesgo.

En este sentido, la acción de *habeas data* constituye el instrumento procesal más eficaz para la garantía del derecho a la intimidad en su dimensión de tutela de los datos personales. A nivel de derecho sustantivo, se concreta en la efectividad del derecho de acceso. En virtud de esta acción y de este derecho el interesado puede obtener el conocimiento necesario de los datos que el responsable de un tratamiento está llevando a cabo. Solo a partir de esta información podrá tener control real sobre los datos que le conciernen, quien los utiliza y para qué. El *habeas data* es la garantía básica para ejercer la autodeterminación informativa que radica en la base del derecho a la protección de datos. Como apunta PÉREZ-LUÑO ROBLEDO, E. C. (2017), esta garantía resulta de capital importancia y es que, en ocasiones, solo a través de ella se puede llegar a tener verdadera constancia de así se está produciendo

un cruce de ficheros, una actividad de perfilado o un uso de los datos acorde al fin para el que se facilitaron.

En relación con la cuestión abordada en este estudio, señala el citado autor que, si bien la doctrina estaba dividida en cuanto a sí el derecho de acceso debía incluir o no las comunicaciones a terceros, la jurisprudencia se ha decantado por que sí se incluyera, por cuanto es la única manera de garantizar el conocimiento de la finalidad última a la que se han aplicado los datos tratados por parte del interesado y permitir así el ejercicio de la autodeterminación informativa. El *habeas data* es la garantía de que los responsables del tratamiento utilicen los datos para el cumplimiento de los fines que legitimaron en inicio de dicho tratmiento.

Siendo esto así, sostengo que el tratamiento de las cesiones intragrupo de los datos personales en grupos de empresa con actividades conjuntas o semejantes, lo que cobraría verdadero sentido sería potenciar este derecho, entendiendo que su alcance no se limite a los datos tratados por el responsable al que se dirige la petición, sino que se informe del tratamiento completo en su conjunto realizado por todas las entidades del Grupo de Empresas; es decir el cumplimiento a nivel de grupo. Esta información sería la misma que se debe facilitar antes del inicio del tratamiento. En consecuencia, si admitimos que un *habeas data* así planteado puede ser más garantista de los derechos del interesado, por qué no seguir el mismo esquema cuando se trata de facilitar la información al inicio de la relación contractual.

4.4. El paralelismo con los tratamientos de la Administración Pública.

Mediante Sentencia 292/2000, de 30 de noviembre, del Pleno del Tribunal Constitucional, dictada en el recurso de inconstitucionalidad 1463/2000, promovido por el Defensor del Pueblo respecto de los arts. 21.1 y 24.1 y 2 de *la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal*, el TC declaró la nulidad de la parte del artículo 21 de la LOPD, que consideraba suficiente para la cesión de datos entre administraciones, que lo previera la disposición de creación del fichero, que bien podría ser una norma con rango inferior a la ley.

El legislador llegó a considerar adecuada la cesión articulada a través de la norma de creación del fichero, que no tenía por qué tener rango de ley. Esta cuestión fue debatida en

sede judicial y se llegó a considerar excesiva la cesión de datos basada en una norma de rango inferior a la ley. Actualmente en el ámbito de las Administraciones Públicas, se establece la posibilidad de que se produzca cesión de datos personales entre administraciones sin consentimiento del interesado cuando se trate del ejercicio de las mismas competencias o de competencias distintas que versen sobre la misma materia. Se contempla la cesión interadministrativa sin consentimiento cuando el destino de los datos comunicados sea el tratamiento con fines históricos, estadísticos o científicos y se permite igualmente cuando se trate de datos personales que una Administración Pública recabe con destino a otra. Es evidente que la Administración es un sujeto obligado *sui generis* frente a la que decaen o pierden fuera muchos derechos del interesado; todo ello, además, partiendo que de estas especialidades derivan de una ley (que no tiene por qué ser Ley Orgánica), y como supuesto excepcional que es no se puede plantear una aplicación total por analogía de este modelo, pues va contra las más elementales normas de interpretación del Derecho; pero sí se podrían aprender lecciones del funcionamiento de este modelo. Permitir determinadas cesiones entre administraciones es práctico, eficiente; y se entiende que suficientemente garantita de los derechos de los interesados, puesto que de otro modo no resultaría admisible ni siquiera en el ámbito de la Administración.

En definitiva, se trataría de definir un planteamiento similar en parte, mediante refrendo legal necesario, para el tratamiento de datos en el seno de grupos de empresa con procesos alineados, predefinidos por la matriz (o la unidad de control) y cuyos tratamientos presenten escaso riesgo para los derechos de los interesados. La cuestión se ceñiría a delimitar qué tipos de empresa podrían acceder a un régimen de cesión intragrupo de base legal, sin necesidad de articular acuerdos intragrupo adicionales con carácter general y definir los requisitos necesarios para aplicar este régimen. Del mismo modo que las distintas normas legales atributivas de potestades a las administraciones les ofrecen un margen importante para la realización de las comunicaciones que son imprescindibles y útiles para los ciudadanos, podría pensarse en un esquema similar, basada en un único acto informativo del tratamiento a nivel de grupo de un determinado tipo de grupos de empresa, que bien podrían ser aquellos que desarrollan una actividad concreta a través de varias entidades que actúan de forma sincronizada.

4.5. Otros sectores del ámbito del *compliance*:

Con carácter general, desde 2010 se ha producido en nuestro país un desarrollo notable del área del derecho que es otros países es conocida como "*compliance*" y que abarca una serie de actividades y conductas susceptibles de acarrear sanciones penales para las empresas. Una de dichas conductas es la relativa al cumplimiento de la normativa de protección de datos, pero hay muchas más, como puede ser el cumplimiento de la normativa de prevención del blanqueo de capitales o la normativa en materia de lucha contra la corrupción empresarial y, en términos generales, la competencia desleal (que es el criterio común de todos los delitos de los que puede responder penalmente una persona jurídica en nuestro país).

Si bien la responsabilidad penal de las personas jurídicas nació en nuestro ordenamiento el 23 de diciembre de 2010 con la entrada en vigor la *Ley Orgánica 5/2010 de reforma del Código Penal*, no ha sido hasta el 1 de julio de 2015 —con la entrada en vigor de la *Ley Orgánica 1/2015, de reforma del Código Penal*—, que se ha regulado expresamente la exención de responsabilidad criminal a la persona jurídica que fomente un comportamiento de cumplimiento entre sus empleados, mediante el desarrollo de un modelo de organización y gestión eficaz.

A la luz de estas modificaciones normativas producidas en materia penal, es frecuente ya encontrar Grupos de Empresas que han desarrollado un plan de cumplimiento para la prevención de la comisión de delitos, y han compilado los procedimientos y controles que tienen para la efectiva prevención y mitigación de riesgos, especialmente los penales. Todos estos procesos, planes y medidas quedan recogidos en un sistema o programa de cumplimiento cuyo ámbito de aplicación es el Grupo Empresarial en su conjunto, como no podría ser de otro modo abarcando todos los procesos existentes, incluida la protección de datos.

El desarrollo de estos programas de cumplimiento normativo o *compliance* ha sido liderado por profesionales especializados en la aplicación de esta materia en sus diferentes facetas: abogados, consultores, empresas de certificación.... y el enfoque es muy similar al del RGPD: parte del análisis de procesos identificación de riesgos y diseño de medidas de contención. Es decir, no hay una regulación detallada de cómo se ha de aplicar el sistema de

cumplimiento; simplemente hay una responsabilidad proactiva y si se demuestra la aplicación y eficacia del sistema, llegado el caso, podrá ser de aplicación la eximente prevista en el Código Penal.

En algunas áreas concretas del *compliance*, como puede ser la prevención del blanqueo de capitales, la propia norma reguladora (Ley 10/2010 de 28 de abril de prevención del blanqueo de capitales y de la financiación del terrorismo) ya prevé que los sujetos obligados aprobarán una serie de políticas y procedimientos de control interno que serán obligatorios para todas las filiales que a su vez sean sujetos obligados (incluso en el extranjero); y expresamente indica que "*En los grupos que integren varios sujetos obligados, el representante será único y deberá ejercer cargo de administración o dirección de la sociedad dominante del grupo"* (artículos 26 y 26 ter de la citada ley 10/2010 de 28 de abril). Es decir, todos los procedimientos se aplicarán a nivel de grupo.

Y de forma similar, en la lucha contra la corrupción, se ha ido imponiendo el modelo de autorregulación ética de las empresas para que éstas se decidan por sí mismas a controlar sus riesgos. Pero el enfoque es siempre global, parte de un proceso de análisis de riesgos y definición de controles y nace normalmente de una política empresarial, un código de conducta y una serie de políticas empresariales que siempre se aplican al nivel del Grupo de Empresa, desde la alta dirección. No cabe pensar en otra estructura pues no tendría ningún sentido hacerlo. El concepto de Grupo Empresarial es un término definido y empleado en multitud de áreas del derecho para delimitar el ámbito subjetivo de aplicación de las normas; y en ninguna de estas disciplinas se deja de emplear por el único motivo de que el fundador optó por una estructura societaria formada por varias entidades.

De hecho, el concepto de grupo de empresa no es del todo ajeno a la protección de datos, gozando de un reconocimiento en el ámbito de las transferencias internacionales, en relación con las cuales aquellos grupos que dispongan de reglas corporativas vinculantes aprobadas por la Comisión gozarán de autorización para la realización de transferencias internacionales. Este planteamiento de cumplimiento a nivel de grupo de las obligaciones y medidas de seguridad en la transmisión de datos bien podría servir de base para garantizar la eficacia de la autodeterminación informativa del interesado, informando de las prácticas a nivel de grupo y de qué entidades tratan qué datos con finalidades comunes todo ello, mediante políticas y procedimientos conjuntos y globales.

5. Conclusiones

I. Con carácter general, y salvo en el ámbito de las actividades reguladas, toda persona tiene libertad para llevar a cabo una actividad comercial, pudiendo organizarla del modo que mejor convenga a sus intereses. Para ello, existen múltiples figuras a tal fin, cada una con un régimen y particularidades propias. Ahora bien, a medida que estas sociedades se consolidan y empiezan a crecer, es frecuente que se organicen como grupos de empresa.

II. Desde el punto de vista estrictamente normativo la articulación de los flujos de datos dentro de un grupo de empresas no es una cuestión baladí. En función del flujo existente y de la estructura del grupo variará el análisis teórico de las diferentes maneras de articular los flujos de datos personales dentro del grupo de empresas; cada uno con sus requisitos y consecuencias propias.

III. El esquema del encargo de tratamiento, acaso el más extendido en la práctica para la regulación de relaciones a efectos de protección de datos en grupos de empresas, es aquel en que una empresa es responsable de los datos que otra procesa por cuenta de aquel. El RGPD desgrana exhaustivamente este modelo de tratamiento, al punto de permitir la utilización de modelo contractual prácticamente estándar. Es, además, un modelo que supone una simplificación los requisitos informativos al interesado. Sin embargo, no siempre se da la premisa básica necesaria para su aplicación, que no es otra que sea el responsable quien decida sobre medios y fines. En los grupos de empresa no es extraño que sea el prestador del servicio el que decide sobre estos extremos.

IV. El esquema de la corresponsabilidad parte de la existencia de un tratmiento con decisión conjunta sobre medios y fines. La norma no especifica con detalle qué ha de entenderse por decisión conjunta, pero en principio se ha de entender que se trata de una decisión consensuada sobre medios y fines entre dos o más personas (Supervisor de Protección de Datos de la Unión Europea; 2019). Y aun así el concepto sigue en evolución identificándose alguna interpretación que lo aborda como la confluencia de responsables y tratamientos, sin que concurra necesariamente un consenso sobre los medios y fines (Autoridad de Control Alemana, 2020). No es un paradigma de uso habitual, entre otras cosas porque al contrario de lo que sucede con la figura del encargado, la regulación es escasa, los requisitos informativos necesariamente se complican por la naturaleza misma

de la coexistencia de responsables y el régimen de responsabilidad frente a terceros se complica.

V. El último tipo de instrumento existente para la transmisión de datos entre compañías del mismo grupo es la cesión de datos. Ello conlleva una carga importante de gestión interna pues requerirá articular correctamente todas las bases legitimadoras del tratamiento, incluido el consentimiento, llegado el caso; y eleva los requisitos informativos exigibles frente a los interesados, que ven como sus datos se trasvasan de una empresa a otra dentro del mismo grupo empresarial. Articular los flujos de datos dentro de los grupos de empresa es engorroso y no necesariamente sirve al propósito de una mayor transparencia y eficacia en la protección de los derechos de los interesados.

VI. Con este panorama, los Grupos de Empresas que necesitan utilizar datos comunes en el seno de sus organizaciones para el desarrollo de su actividad afrontan una cierta sobrecarga burocrática, especialmente las pequeñas y medianas empresas, que en España representan aproximadamente el 99% del tejido productivo; y parte de ellas son Grupos de Empresas afectados por la problemática expuesta.

VII. Llegados a este punto vale la pena plantearse si no habría una forma más garantista y eficiente que la de aplicar la normativa de forma independiente a cada empresa dentro de un Grupo de Empresas; un planteamiento en que en ningún caso redundara en perjuicio de los interesados respecto del sistema actual.

A este respecto, hay que tener en cuenta que la Comisión apunta a la consolidación del enfoque metodológico basado en el riesgo como el camino óptimo para encontrar una solución que permita dar cumplimiento a la norma y garantizar los derechos de los interesados sin sobrecargar innecesariamente a los sujetos obligados, incidiendo en que "*el tamaño no es en sí mismo una indicación de los riesgos que el procesamiento de datos personales cuyo cumplimiento deficiente puede conllevar para individuos*" (*Commission Staff Working Document accompanying the documment Communication from the Commission to the European Parliament and the Council; 2020*). En efecto, el enfoque basado en el riesgo permite combinar flexibilidad con protección efectiva; y esto se podría predicar tanto de las pymes como de las grandes empresas.

Asimismo, del análisis de la Comisión, cabe concluir que es legítimo buscar la fórmula que permita flexibilizar la aplicación de la norma para dar solución y cobertura a todos los riesgos que existan en materia de protección de datos, pero sin sobrecargar o exigir

una cantidad de recursos desproporcionada cuando dichos tratamientos apenas conlleven riesgo.

VIII. Desde otro punto de vista, para garantizar la inexistencia de un perjuicio del interesado en un esquema diferente es necesario reforzar las garantías del interesado y como exponente esencial de ellas en este asunto en concreto, el habeas data. Es la garantía capital a través de la cual se puede llegar a tener verdadera constancia de sí se está produciendo un cruce de ficheros, una actividad de perfilado o un uso de los datos acorde al fin para el que se facilitaron (PÉREZ-LUÑO ROBLEDO, E. C.; 2017).

IX. En el ámbito de la administración no llama la atención la cesión entre administraciones de datos necesarios para el cumplimiento de los fines previstos. Salvando las distancias es un paralelismo con lo que puede suceder dentro del ámbito empresarial. En el caso de las administraciones la base sobre la que se articula la cesión en la existencia de una norma con rango de ley; de forma similar se podría articular para permitir el intercambio de datos en grupos de empresas, con garantías suficientes, reforzando el derecho de acceso y el habeas data en una propuesta de *lege ferenda*.

X. El cumplimento de la normativa de índole regulatoria a nivel de grupo de empresa es una tendencia consolidada en otras áreas del derecho, que de facto aporta más garantías de buen funcionamiento y más transparencia, especialmente en ámbitos regulados; así sucede en áreas tales como la prevención del blanqueo de capitales, el régimen fiscal, los sistemas de cumplimiento penal y políticas anticorrupción; todos ellos partes de una visión global de la empresa formada por diversas entidades jurídicas independientes pero con una unidad de decisión conjunta, evitando una fragmentación del cumplimiento de la norma.

XI. Así las cosas, con un enfoque basado en el riesgo, identificando no ya entidades jurídicas que llevan a cabo actividades, sino los procesos globales en los que intervienen las diferentes entidades pertenecientes a un mismo Grupo de Empresas se podría articular un sistema de cumplimiento de la normativa de protección de datos a nivel de grupo, con una serie de requisitos mínimos en garantía de los derechos de los interesados tales como:

1. Identificación de procesos para los que se recaban y tratan los datos. No puede darse un cruce de datos para distintos procesos sin consentimiento (u otra base

legitimadora); pero, dentro del desarrollo del proceso, aun si intervienen diferentes entidades del grupo de empresas, sí podría establecerse un flujo libre;

2. Información completa y clara del proceso y del tratamiento de los datos del interesado en el momento inicial del tratamiento (y siempre a su disposición; pero sin necesidad de información supletoria con ocasión de cada cesión intragrupo); cediendo en importancia la identificación de la entidad que trata el dato, a cambio de una mayor delimitación de las líneas rojas marcadas por el uso autorizado; y
3. Existencia de un único responsable último frente al interesado; que deberá ser la unidad de decisión última del proceso en cuestión; sin necesidad de múltiples responsables o regímenes de responsabilidad compartida o fragmentada.

XII. En cualquier caso, a día de hoy no es esta la postura del Tribunal Supremo y en tanto no se articule con apoyo legal de otro modo un cambio de modelo, cada flujo de datos intragrupo habrá de ser identificado y encajado en la tipología existente en la normativa para el trasvase de datos entre compañías, como cesión, encargo de tratamiento o tratamiento corresponsable, y regulando con la profusión necesaria todos los protocolos y acuerdos alrededor del tratamiento que sean necesarios para no incurrir en falta frente a la autoridad de control. Esto puede resultar en una sobredosis informativa al interesado y, sin duda una sobrecarga para los sujetos obligados, especialmente gravosa en el caso de las empresas medianas.

Referencias bibliográficas

Bibliografía básica

CAVERO, P.G. Las políticas anticorrupción en la empresa*. Revista De Derecho*, 2016, no. 47. págs. 219-244 ProQuest Central.

LUCAS MURILLO DE LA CUEVA, P. (2007). «Perspectivas del derecho a la autodeterminación informativa». En: «III Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas». IDP. Revista de Internet, Derecho y Política. N.º 5. UOC.

RALLO LOMBARTE, A. Hacia un nuevo sistema europeo de protección de datos: las claves de la reforma. UNED. *Revista de Derecho Político* N.º 85, septiembre-diciembre 2012, págs. 13-56.

RODRÍGUEZ AYUSO, J. F. (2019). *Figuras y responsabilidades en el tratamiento de datos personales*. J.M. BOSCH EDITOR. pág. 92

SCHÜTZE, B., KÄMMERER, M. Teleradiología legal: Implementación de requisitos de protección de datos. *Radiólogo* 59, págs. 637-642 (2019).

PÉREZ-LUÑO ROBLEDO, E. C. (2017). *El procedimiento de habeas data: el derecho procesal ante las nuevas tecnologías.* Dykinson; pág. 148).

VALDIVIESO LÓPEZ, E. (2012). Los criterios de vinculación y la responsabilidad solidaria en los grupos de empresas. A propósito de una casación en materia laboral. *Revista de Investigación Jurídica. IUS. 02*(3), 2012. Red Universidad Católica Santo Toribio de Mogrovejo. (pág. 13)

Bibliografía complementaria

- *Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder – 12.05.2020 Hinweise zum Einsatz von Google Analytics im nicht-öffentlichen Bereich* (Dictamen de la Conferencia de Supervisores Independientes de Protección de Datos de los gobiernos federales y estatales – 12 de mayo de 2020. Notas sobre el uso de *Google Analytics* en el sector privado).

- *Commission Staff Working Document* —SWD(2020) 115 final— *accompanying the document Communication from the Commission to the European Parliament and the Council* — COM(2020) 264 final— *2020; págs 25.26*
- Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento». 16 de febrero de 2010.264/10/ES WP 169
- EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725. Supervisor Europeo de Protección de Datos. 11 noviembre 2019. (https://edps.europa.eu/data-protection/our-work/our-work-by-type/guidelines_en) [ultima consulta 8 de julio de 2020].
- Guidelines on Transparency under Regulation 2016/679. GT29 (17/EN WP260 rev.01)
- Informe 0325/2004 Gabinete Jurídico AEPD. 2004.
- Informe 0245/2010 Gabinete Jurídico AEPD. 2010.
- Informe 0010/2014 Gabinete Jurídico AEPD. 2014.
- Informe 0175/2018 Gabinete Jurídico AEPD. 2018.
- Ministerio de Trabajo. Cifras Pyme 2019. (http://www.ipyme.org/es-ES/ApWeb/EstadisticasPYME/Documents/CifrasPYME-enero2019.pdf) [ultima consulta 8 de julio de 2020].
- Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. Working Party 29. 9 de abril de 2014. 844/14/EN WP 217.

Legislación citada

- Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos;
- Reglamento (UE) 2014/651 de la Comisión, de 17 de junio de 2014, por el que se declaran determinadas categorías de ayudas compatibles con el mercado interior en aplicación de los artículos 107 y 108 del Tratado
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)

- Corrección de errores del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)
- Real Decreto de 22 de agosto de 1885, por el que se publica el Código de Comercio.
- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
- Ley Orgánica 15/1999 de 13 diciembre de 1999 de Protección de Datos Personales
- Ley 10/2010 de 28 de abril de prevención del blanqueo de capitales y de la financiación del terrorismo;
- Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995 de 23 de noviembre del Código Penal
- Ley Orgánica 1/2015, de 30 de marzo por la que se modifica la Ley Orgánica 10/1995 de 23 de noviembre, del Código Penal
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.

Jurisprudencia referenciada

TSJ Madrid (Contencioso), Sec. 9ª, 16 octubre 2000, nº 848/2000, Rec. 1132/1997

TS sala 3ª, Sec. 6ª, 18 octubre 2000.Rec. 423/1996

Audiencia Nacional (Contencioso), Sec. 1ª, 24 junio de 2010, Rec. 425/2009

Listado de abreviaturas

AEPD: Agencia Española de Protección de Datos

CC. Código civil

CCo. Código de comercio

Directiva 95/46/CE: Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

LOPD: Ley Orgánica 15/1999 de 13 diciembre de 1999 de Protección de Datos Personales

LOPDGDD: Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales

Pág.: Página

Rec.: Recurso

RGPD: Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

TC: Tribunal Constitucional

TS: Tribunal Supremo

TSJ: Tribunal Superior de Justicia

Vid.: Véase