Universidad Internacional de La Rioja

Facultad de Derecho

Máster Universitario en Protección de Datos

El Principio de Responsabilidad Proactiva en el Reglamento General de Protección de Datos

Trabajo fin de estudio presentado por:	María Ángeles Cañavate Megías
Tipo de trabajo:	Trabajo Fin de Máster
Directora:	Dña. Elena Davara Fernández de Marcos
Fecha:	21/07/2021

Resumen

El principio de responsabilidad proactiva, conocido como *accountability* en inglés, constituye la base del modelo de protección de datos personales implantado por el Reglamento General de Protección de Datos. Se trata de un principio general de derecho específico en materia de protección de datos personales, que actúa como garantía del cumplimiento del resto de los principios aplicables en esta materia, con proyección en la interpretación y aplicación de todo el Reglamento General de Protección de Datos. Se introduce así en la norma un concepto jurídico indeterminado de extraordinaria importancia y amplitud.

En el presente trabajo se abordará el problema que puede suponer en la práctica la interpretación de este concepto jurídico indeterminado, sobre todo para sectores no especializados del derecho. Se aspira a concretar su significado, su alcance y las obligaciones que genera. Para ello, se estudiará tanto el principio de responsabilidad como los elementos esenciales que forman parte del modelo de protección. Con ello, se pretende contribuir en reducir la inseguridad jurídica.

Palabras clave: «Responsabilidad proactiva», «Modelo preventivo», «Privacidad desde el diseño», «Privacidad por defecto», «Delegado de Protección de Datos».

Abstract

The *accountability* principle is the basis of the date protection model established by the General Data Protection Regulation. It is a general principle specific to the field of personal data protection that serves to guarantee the observance of the other applicable principles in this field, and which permeates the interpretation and implementation of the entire General Data Protection Regulation. A new undefined legal concept with outstanding importance and magnitude is thus introduced in the norm.

This work addresses the issues that may entail, in practice, the interpretation of this undefined legal concept, mainly for non-legal practitioners. It aims to delineate its significance, its scope and the obligations it creates. To do so, it analyses the principle itself, as well as the essential elements which together form the protection model. The ultimate objective is to contribute to reducing the legal uncertainty.

Keywords: «*Accountability*», «Preventive Model», «Privacy by design», «Privacy by default», «Data Protection Officer».

Índice de contenidos

1. Introducción

La entrada en vigor 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», en adelante RGPD, «representa un verdadero cambio de paradigma» (CAMERO, 2019, p.1) en esta materia.

Los motivos de este cambio no son otros que los que motivaron al legislador europeo a iniciar la reforma de 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, en adelante Directiva 95/46/CE. En un contexto social cambiante a pasos agigantados debido a «la rápida evolución tecnológica y a la globalización» (considerando 6 RGPD[1]), se requería de una norma cuya declaración de principios y obligaciones de protección de datos personales se reflejara «en medidas internas y prácticas concretas». Había que pasar «de la teoría a la práctica» (GT29[2]. WP173. pp.1 y 3).

Lo que empezó siendo una reforma para la actualización de la Directiva 95/46/CE acabó con la aprobación del RGPD. El Reglamento resultó ser un instrumento legislativo más acorde con la gran envergadura de la reforma pretendida y, dada su aplicabilidad directa, permitía resolver la divergencia de regulaciones nacionales (considerando 9 RGPD[3]) a que dio lugar la transposición de la Directiva 95/46/CE en los países de la Unión Europea –UE–.

El RGPD ha diseñado un nuevo sistema de protección de datos personales basado en la prevención. La Directiva 95/46/CE ha sido derogada y, con ello, su particular modelo de cumplimiento esencialmente reactivo. Con el RGPD «pasamos de una responsabilidad 'reactiva' a una 'proactiva'» (DAVARA, 2020, p. 131). Ahora, se requiere una actitud proactiva[4]

[1] En el considerando 6 RGPD se hace referencia a los «nuevos retos» para la protección de datos que originaron la adopción del RGPD.
[2] El Grupo de Trabajo del Artículo 29 (GT29) era el órgano consultivo independiente creado en virtud del art. 29 de la Directiva 95/46/CE. Ahora sus funciones han sido asumidas por el Comité Europeo de Protección de Datos.
[3] En el considerando 9 RGPD se explican los problemas que la Directiva 95/46/CE no pudo solucionar.
[4] El considerando 85 del RGPD hace referencia a la actuación activa, que debe tener el responsable del tratamiento en la notificación de brechas de seguridad.

que permita anticiparse a los posibles incumplimientos, con el fin de aplicar medidas eficaces que eviten que dichos incumplimientos lleguen a producirse.

Los cimientos que sustentan este nuevo modelo son el principio de responsabilidad proactiva[5] o *accountability* en inglés, un enfoque de la seguridad basada en los riesgos, el principio de protección desde el diseño y por defecto y el Delegado de Protección de Datos. El factor clave para el buen funcionamiento de este engranaje es el principio de responsabilidad proactiva.

Llama la atención que en todo el RGPD, a pesar de su enorme importancia, el término responsabilidad proactiva solo aparece dos veces[6] y que tampoco contiene su definición[7] . Sin embargo, este principio irradia todo el RGPD como lo evidencia el hecho de que los términos que lo definen, como cumplir y demostrar entre otros, se repiten una y otra vez[8] a lo largo de su texto. Esto es debido a que el legislador europeo ha recurrido a la técnica legislativa de introducir un principio de derecho, con la intención de que la norma resultante sea lo suficientemente flexible y pueda así adaptarse a los casos concretos, aunque estos sean sustancialmente diferentes. Se pretende evitar un cumplimiento meramente formal[9] y se opta por la introducción de una obligación de resultado, cumplir y ser capaz de demostrarlo «responsabilidad proactiva» (art. 5.2 RGPD).

De este modo, se da la circunstancia de que el elemento clave para la correcta interpretación y cumplimiento del RGPD, la *accountability*, podría ser su principal obstáculo. Esto es así debido a que se trata de un concepto jurídico indeterminado, un principio general de derecho en esta materia, cuya característica es precisamente la imprecisión o vaguedad.

La contribución de este TFM es facilitar la compresión de este principio de responsabilidad proactiva. Se pretende realizar una explicación sencilla y escueta que sirva de ayuda a los diferentes sectores, especializados o no en el derecho. Para ello, mediante un trabajo de síntesis y análisis jurídico, se tratará de concretar su significado, su alcance y las obligaciones que genera.

---

[5] En este TFM nos referiremos indistintamente al principio de responsabilidad proactiva o *accountability.*
[6] En el considerando 85 y en el art. 5.2 del RGPD.
[7] En el art. 4 del RGPD, dedicado a las definiciones, no se define "responsabilidad proactiva".
[8] En el RGPD se repiten los términos que definen el principio de responsabilidad proactiva muchas veces: "cumplimiento" 71 veces, "garantizar el cumplimiento" 12 veces, "cumplir" 25 veces, "demostrar" 21 veces, "demuestra" 3 veces, "demostrar el cumplimiento" 6 veces, "responsabilidad" 23 veces.
[9] La mera adopción de un listado de medidas no garantiza un cumplimiento efectivo.

1.1. Justificación del tema elegido

La justificación de la elección del principio de responsabilidad proactiva como materia de este trabajo es doble.

Por un lado, considero que entender el término *accountability* es esencial para interpretar correctamente el RGPD y la envergadura de la reforma que introduce en la materia. Su compresión puede ilustrarnos sobre la intención del legislador europeo lo cual redundará a su vez en la aplicación adecuada del modelo de protección de datos personales que introduce el RGPD.

Por otro, adentrarse en el terreno de los principios de derecho y conceptos jurídicos indeterminados no es una labor baladí. Para esto, sin duda, se requiere un trabajo profundo de investigación, de análisis jurídico, de síntesis y de comunicación escrita. En definitiva, alcanzar los objetivos de este trabajo supone un gran estímulo.

1.2. Problema y finalidad del trabajo

El problema detectado es que el elemento clave para el correcto cumplimiento del RGPD, la *accountability,* es difícil de entender por tratarse de un concepto jurídico indeterminado, esto es, de un principio de derecho que ha sido introducido en la norma con un significativo grado de imprecisión. . Esto puede suponer un verdadero inconveniente en sectores no especializados del derecho, adicionalmente puede añadir cierto grado de dificultad a los operadores jurídicos.

La finalidad de este TFM consiste en reducir la inseguridad jurídica que puede suponer la interpretación de este concepto jurídico indeterminado. Se pretende facilitar una sencilla y somera explicación que facilite su interpretación y, con ello, la correcta aplicación del RGPD. En definitiva, se aspira a reducir la inseguridad jurídica.

1.3. Objetivos

El objetivo último de este TFM es facilitar el entendimiento y alcance del principio de responsabilidad proactiva. Para ello, y de forma instrumental, nos fijamos la consecución secuencial y ordenada de unos objetivos específicos. Esto nos permitirá desmenuzar y aclarar el problema planteado mediante la lógica jurídica, de forma ordenada y sencilla. El resultado de este análisis será recogido en las conclusiones de este TFM.

Nuestra intención es precisar y concretar un concepto jurídico indeterminado, queremos evitar caer en disquisiciones jurídicas innecesarias que nos llevarían a más imprecisión y confusión. Por ello, nos centraremos únicamente en dos objetivos específicos:

El primer objetivo consiste en explicar el concepto de responsabilidad proactiva. Para ello analizaremos el concepto prestando especial atención a los dos requisitos que lo definen, el requisito de cumplir y el requisito de ser capaz de demostrarlo. Además, se abordarán las obligaciones en que se concreta el cumplimiento efectivo de este principio.

El segundo objetivo viene dado por la idea de sistema del ordenamiento jurídico, la cual nos lleva a interpretar el principio de responsabilidad proactiva en el contexto del modelo de protección implantado por el RGPD. Por tanto, es imprescindible abordar también el cambio de enfoque en materia de seguridad, la privacidad desde el diseño y por defecto y el Delegado de Protección de Datos. Como veremos, estos elementos están estrechamente relacionados con la *accountability* y juntos contribuyen al correcto cumplimiento del RGPD.

2. Nuevo modelo de privacidad introducido por el RGPD

Como hemos indicado, la característica más relevante de la entrada en vigor del RGPD es que supone el cambio del modelo de protección de datos personales vigente en la UE desde la aprobación de la Directiva 95/46/CE, caracterizado por ser esencialmente reactivo. El RGPD incorpora un modelo preventivo, si bien esto no obsta para que también siga presente la reacción ante el incumplimiento. El RGPD «ha diseñado una *potente estrategia preventiva*, que, mediante pluralidad de mecanismos e instrumentos, materializa las exigencias básicas del *accountibility principle*» (RALLO, 2012, p. 50). Este modelo es sustentado principalmente por cuatro elementos: 1. El enfoque en los riesgos en materia de seguridad. 2. El principio de protección desde el diseño y por defecto. 3. El Delegado de Protección de Datos. 4. El principio de responsabilidad proactiva.

Sobre la seguridad enfocada en los riesgos. La Directiva 95/46/CE ya imponía a los responsables del tratamiento, en su art. 17, como también hace el RGPD, la obligación de adoptar medidas de seguridad adecuadas para la protección de los datos personales teniendo en cuenta los conocimientos técnicos existentes y el coste de su aplicación. Con la Directiva 95/46/CE el nivel de seguridad exigido era el que fuera más apropiado atendiendo a los riesgos del tratamiento y a la naturaleza de los datos personales. La naturaleza de los datos personales venía a determinar qué medidas de seguridad eran las adecuadas para la protección. Dicho de otra manera, el nivel de riesgo venía dado por la categoría de datos personales objeto de tratamiento. Con ello, se ponía el foco en los tipos de datos. Esto es lo que ha cambiado. El RGPD ha desplazado el foco de los tipos de datos a los riesgos potenciales.

Desde un punto de vista práctico, si lo comparamos con la situación actual, el cumplimiento de los requerimientos en materia de seguridad de la Directiva 95/46/CE era relativamente fácil. A los responsables no se les pedía una reflexión constante sobre si la medida era o no la más adecuada para garantizar la seguridad de los datos personales. Estos ya cumplían con la simple adopción de las medidas que 'tocaran' de la lista de medidas previstas en la norma, cuya elección realizaban esencialmente en función del tipo de datos personales objeto de tratamiento. Pues bien, dada su importancia reiteramos, el RGPD pone el foco en los riesgos –no en los tipos de datos– y exige que se adopten las medidas de seguridad que sean las más

adecuadas atendiendo a los riesgos de probabilidad y gravedad variables[10] y, además, que lo sean en todo momento. De esta forma, el análisis de riesgos es configurado como la herramienta clave para decidir en materia de seguridad.

En España, la transposición de la Directiva 95/46/CE se realizó con la aprobación de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal[11], en adelante LOPD. A su vez, en 2007 se aprobó el Real Decreto 1720/2007[12], de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, en adelante RLOPD. Este reglamento estableció tres niveles de medidas de seguridad[13], básico, medio y alto, en función del tipo de datos objeto de tratamiento.

Este marco normativo contribuyó a una suerte de cumplimiento de 'maquillaje' –en el sentido de apariencia de cumplimiento–.Una vez adoptadas las medidas de seguridad, se entendía que ya se había cumplido con los requerimientos de la norma, pero nada garantizaba que las medidas fueran realmente suficientes y adecuadas. Este efecto negativo es el que pretende evitar el RGPD con la seguridad enfocada en los riesgos.

El segundo elemento es el principio de protección desde el diseño y por defecto[14]. Para definir su objetivo podríamos decir que 'no hay mejor medida que la prevención'. El RGPD pretende ir a la raíz de los potenciales problemas. Introduce el principio de privacidad desde el diseño, *privacy by design* en inglés –PbD–, como una apuesta clara por un modelo de protección que tenga en cuenta la protección de los datos personales desde las 'fases iniciales' de cualquier proyecto. Este es el momento en el que hay que actuar –al principio–, cuando se determinan los fines y los medios –aunque también en el momento del propio tratamiento–, mediante la aplicación de las primeras medidas de seguridad tendentes a garantizar el cumplimiento efectivo del RGPD. Además, introduce el principio de protección por defecto– PDpD–, *privacy by default* en inglés, que obliga a los responsables a implementar medidas de seguridad que

[10] Véase art.32 RGPD- Seguridad del tratamiento.
[11] Derogada por la Disposición derogatoria única de la LOPDGDD.
[12] El RD 1720/2007 no ha sido derogado expresamente por la LOPDGDD. Sigue en vigor en todo lo que no contradiga, se oponga o resulte incompatible con el dispuesto tanto en el RGPD como en la LOPDGDD (punto 3, Disposición derogatoria única de la LOPDGDD).
[13] Artículo 80 del RD 1720/2007.
[14] Véase art. 25.1 RGPD -Privacidad desde el diseño- y art. 25.2 RGPD -Privacidad por defecto-.

'por defecto' –sin intervención humana– garanticen la aplicación del principio de minimización a la cantidad de datos personales, a la extensión del tratamiento, al plazo de conservación y a la accesibilidad.

En tercer lugar, y no por ello menos importante, el Delegado de Protección de Datos –DPD–, *Data Protection Officer* –DPO– en inglés. Se trata de una figura crucial para el correcto funcionamiento de este modelo de protección. El DPD ya estaba contemplado en la Directiva 95/46/CE, aunque de forma voluntaria. El RGPD ha elevado al DPD a la categoría de esencial mediante la asignación de importantes funciones, de una posición en la organización al más alto nivel y de un estatus de total y efectiva independencia. Además, el nombramiento del DPD es obligatorio en una serie de supuestos y, en el resto, es altamente recomendable como veremos. El DPD es «la persona con conocimientos especializados del Derecho y la práctica en materia de protección de datos»[15] que desempeña la trascendente tarea de ayudar, tanto a responsables como encargados del tratamiento, en la supervisión de la observancia interna del cumplimiento del RGPD.

Finalmente, la introducción del principio de responsabilidad proactiva en el RGPD es la apuesta definitiva por este principio (DURÁN, TRONCOSO, 2021, tomo I, p. 1788). El legislador europeo ha seguido las recomendaciones aportadas por el GT29, en varios documentos de trabajo, durante el proceso de reforma de la Directiva 95/46/CE. En un primer momento, el GT29 propuso la introducción de la *accountability* como una posible solución a los problemas[16]a que había dado lugar la transposición de dicha Directiva y que motivaron su reforma (GT29. WP168[17]. p.20). Más tarde, en 2010, volvería a abordar el asunto con un estudio pormenorizado de la *accountability* –Dictamen 3/2010 sobre el principio de responsabilidad[18]–. En definitiva, este principio de derecho ha sido integrado en la norma con una singular relevancia, pues viene a actuar como el eje sobre el que gira el modelo de protección del RGPD.

[15] Considerando 97 RGPD.
[16] Entre los diversos problemas, destaca la falta de efectividad de las medidas de seguridad, la excesiva burocracia y la divergencia regulatoria en los diferentes países de la UE.
[17] WP 168 sobre el Futuro de la Privacidad.
[18] WP 173.

2.1. PRINCIPIO DE RESPONSABILIDAD PROACTIVA

En este apartado analizamos la *accountability* en tanto que principio general de derecho específico en la materia de protección de datos. Esto nos ayudará a comprender su significado y alcance.

Los principios jurídicos «son algo ambiguo y difícil de delimitar» (DE CASTRO, 2002, p. 265). El debate doctrinal sobre sobre la distinción entre reglas y principios dista mucho de estar resuelto. En cualquier caso, en cuanto a lo que a nosotros interesa –para explicar el significado y alcance de la *accountability*–, nos centraremos en los aspectos en que la opinión doctrinal es pacífica. La doctrina coincide en que hay una serie de caracteres propios de los principios que los diferencian del resto de normas. A continuación, señalaremos la conexión del principio de responsabilidad proactiva con algunos de estos rasgos definitorios de los principios. Para ello, nos apoyaremos en el trabajo de síntesis realizado por la doctrina (DE CASTRO. 2002).

Los principios son 'fundamentales', fijan las razones para la acción –sus fundamentos–. De esta forma, definen el motivo de realizar o de evitar una determinada conducta. El principio de responsabilidad proactiva establece, para los responsables del tratamiento, una serie de obligaciones –un comportamiento determinado de hacer o de abstenerse– con el fin de cumplir con el RGPD y de demostrar dicho cumplimiento –ésta es la razón–. Por tanto, esta característica es atribuible a la *accountability*. Estamos ante un principio 'fundamental' en materia de protección de datos que debe guiar la actuación del responsable del tratamiento, actuación que viene motivada por el cumplimiento de la norma y la capacidad de demostrarlo.

Los principios son 'generales', ordenan de forma genérica, marcan el límite que no debe ser traspasado. Así, establecen lo que es globalmente considerado aceptable y lo que no. La *accountability* prescribe dos límites generales infranqueables. El primero es el incumplimiento, es necesario cumplir con todos los requerimientos del RGPD. El segundo es la prueba –que es en sí un requerimiento–, debemos poder demostrar en todo momento que hemos cumplido, la falta de prueba se considera un incumplimiento. Por tanto, podemos afirmar que el principio de responsabilidad proactiva es un principio 'general' en la materia.

Los principios 'no son definitivos' o concluyentes, establecen simples directrices que se consideran adecuadas. Por ello, pueden ser cumplidos en diferentes grados. Esta característica aporta al RGPD la flexibilidad necesaria para que el principio de responsabilidad

proactiva pueda ser cumplido en una casuística diversa. Es poco realista pensar que en todas las organizaciones y en todas las situaciones se podrá cumplir con el RGPD exactamente igual. Puesto que la casuística es variada, el grado de cumplimiento también debe serlo. Esto no obsta para que deban ser respetados en todo momento los límites infranqueables mencionados –cumplir y demostrar–. Así pues, podemos afirmar que la *accountability* establece unas directrices de actuación graduables en función del caso concreto.

Los principios son normas 'abiertas' que carecen de la determinación fáctica. Por este motivo, no sabemos claramente cuándo debemos aplicarlas. Además, los principios 'no determinan necesariamente la decisión', pues sólo aportan razones a favor o en contra de las alternativas posibles. Estos rasgos otorgan al principio de responsabilidad proactiva la flexibilidad, antes mencionada, que le permite adaptarse a la diferente casuística.

Los principios tienen una 'dimensión de peso', se trata de una suerte de jerarquía entre ellos. Cuando se produce una colisión entre dos principios, uno de ellos tendrá mayor peso sin que invalide al otro, que también se aplicará, pero en menor grado. El principio de responsabilidad proactiva ha sido introducido explícitamente en el art.5.2 del RGPD como cierre del artículo dedicado a los principios del RGPD. Llama la atención el orden en que se enuncian estos principios. Este orden no es baladí, es importante y tiene una finalidad concreta. Primero se especifican y explican cuáles son los principios relativos al tratamiento (art. 5.1 RGPD). Seguidamente se proclama el principio de responsabilidad proactiva como la garantía del cumplimiento de dichos principios previamente mencionados (art. 5.2 RGPD). Con ello, el legislador ha querido establecer una jerarquía entre el primer grupo de principios y la *accountability*. En consecuencia, todos los principios son importantes, pero se eleva el principio de responsabilidad proactiva a un nivel superior de jerarquía, como guardián del cumplimiento del resto de principios y de todo el RGPD.

Llegados a este punto, tras el análisis de las características arriba mencionadas, podemos afirmar que la *accountability* es también un concepto jurídico indeterminado. Se habla de conceptos jurídicos indeterminados «para señalar a aquéllos cuya formulación resulta más abstracta e imprecisa». La introducción de conceptos vagos es una técnica legislativa –no es impericia técnica– y «a veces se trata de una elección consciente». Por este motivo, «puede señalarse que la expresión conceptos indeterminados alude a una cierta intención de introducir expresiones imprecisas en una norma» (MARTÍNEZ, 2019, pp.163-164).

La intención del legislador europeo con la introducción de la *accountability* en el RGPD –en tanto que principio y con un elevado grado de imprecisión– ha sido la de «favorecer interpretaciones 'adecuadas'» del RGPD y «desacreditar las interpretaciones 'literales'» (COMANDUCCI, 1998, p. 9). Con ello, se pretende huir de la regulación del caso concreto en aras de una mayor aplicabilidad a la casuística en la materia. La intención y el método son loables, pero tiene un inconveniente, con la imprecisión introducimos 'inseguridad jurídica'.

Asimismo, los principios generales del derecho –como la *accountability*– son fuentes del Derecho (art.1º CC)[19] y, además, tienen carácter normativo. Por otro lado, el propio Código Civil pone el acento en la palabra 'normas' – no leyes– cuando aborda la interpretación de estas (art. 3º CC) y en cuyo ámbito están incluidos los principios. En consecuencia, el principio de responsabilidad proactiva –en tanto que principio general del derecho– debe ser interpretado siguiendo todos los criterios interpretativos[20] establecidos en el CC– no sólo el literal–. Además, y al hilo de lo anterior, los principios generales del derecho desempeñan la función de ser fuente supletoria ante laguna, es decir, en defecto de ley y costumbre (REBOLLO, 2011, p.16). Por consiguiente, esto confiere a la *accountability* la cualidad de poder completar posibles lagunas en el RGPD, a través de técnicas como la analogía.

Por último, queremos resaltar la notable «función informadora» (REBOLLO, 2011, p.13) que desempeña la *accountability*, que le viene dada por el art. 1º.4 del CC[21]. Así, se le otorga la tarea de «inspirar, orientar o informar los distintos elementos» del RGPD. Además, va más allá del propio RGPD, se extiende a la LOPDGDD y a toda la normativa sectorial en materia de protección de datos. Esto es debido a la onda expansiva que genera la aplicabilidad directa en todos sus elementos del Reglamento Europeo. Con ello, «queremos llamar la atención» (Davara, 2020, p. 127) sobre el hecho de que el legislador europeo ha elegido esta figura legislativa con la intención de conseguir este efecto expansivo y que esto es también aplicable a la *accountability*.

[19] Véase el art. 1º CC: Las fuentes del derecho son la ley, la costumbre y los principios generales del derecho.
[20] El art. 3 del CC incluye la interpretación literal, la sistemática, la histórica, la sociológica y la teleológica o finalista. Todas ellas son complementarias y no excluyentes.
[21] Véase art. 1.4 CC: Los principios generales del derecho tienen carácter informador del ordenamiento jurídico.

2.1.1. Concepto

En términos generales el concepto de 'responsabilidad' hace referencia a la idea de respuesta para reparar el equilibrio roto. En el ámbito del derecho, el 'concepto jurídico de responsabilidad' deriva de la necesidad de restablecer un equilibrio roto que es considerado como un bien o valor. Un presupuesto imprescindible de la responsabilidad es la libertad de acción del sujeto obligado por la norma. Cuando el sujeto decide libremente, con su elección, también se imputa las consecuencias de sus actos (DE CASTRO, 2002, pp. 357-358).

En el ámbito de la protección de datos personales, el concepto[22] de *accountability* proviene del *Common Law* anglosajón, su traducción a otras leguas no resulta fácil. En español se ha traducido como «obligación de rendir cuentas» (GT29. WP173. p. 8). La rendición de cuentas está incluida en la definición antes dada de responsabilidad jurídica. De forma instrumental, para entender correctamente el término de *accountability*, podemos servirnos del concepto de responsabilidad en derecho español.

Tal cual ha sido configurada la *accountability*, podemos afirmar que estamos ante una responsabilidad objetiva –por resultado–. Es decir, no se requiere el ánimo del sujeto –que haya querido un resultado– para que deba responder por el incumplimiento del RGPD. La *accountability* ha sido regulada sin hacer alusión a la intencionalidad de la acción del responsable. Primero, se establece que el responsable del tratamiento será el responsable del cumplimiento y capaz de demostrarlo – *accountability*– (art. 5.2 RGPD). Posteriormente, mediante una redundancia en la rúbrica del art. 24 del RGPD –responsabilidad del responsable del tratamiento– (DURAN, TRONCOSO, 2021, tomo I, p. 1790) se insiste en la idea de que será el responsable del tratamiento quien deberá responder del cumplimiento del RGPD y, además, deberá ser capaz de demostrarlo –no poder demostrarlo es ya en sí mismo un incumplimiento–.

Adicionalmente, la *accountability* constituye una responsabilidad directa y puede ser también indirecta. Al hilo de lo anterior, no cabe duda de que la responsabilidad directa del responsable del tratamiento es aquella derivada de sus actos contrarios a la norma. Pero el RGPD ha ido más allá, exige al responsable un deber de diligencia en la elección de quienes

[22] A título de recordatorio, a lo largo de este TFM nos estamos refiriendo al principio de responsabilidad proactiva o *accountability* indistintamente.

tratarán los datos personales siguiendo sus instrucciones (art. 28.1 RGPD). La consecuencia es que el responsable del tratamiento deberá responder por los actos de sus encargados –salvo que estos se aparten de las instrucciones recibidas–. Estamos ante la responsabilidad indirecta del responsable por los actos de un tercero.

El legislador europeo ha sido parco en palabras para definir las obligaciones que integran el concepto de *accountability*. Así, en una frase establece que «el responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo» (art. 5.2 RGPD). De este modo introduce los dos requisitos que conforman la responsabilidad proactiva, cumplir y ser capaz de demostrarlo. Posteriormente, lo establecido en el art. 5.2 RGPD es desarrollado en el art. 24 RGPD antes mencionado. El considerando 74 del RGPD aborda la interpretación que debe hacerse de ambos artículos .

A continuación, se analizarán con más detalle los dos requisitos que definen la *accountability*.

2.1.1.1. Requisito de cumplir

Aunque de la literalidad del art. 5.2 RGPD pueda parecer que el principio de responsabilidad proactiva hace referencia únicamente al cumplimiento de los principios del tratamiento mencionados en el apartado 1 de dicho artículo, no es así, se refiere a todo el RGPD. Traemos a colación lo explicado previamente sobre las implicaciones de la *accountability* en tanto que principio general de derecho para la interpretación y aplicación del RGPD.

El principio de responsabilidad no es nuevo. El legislador europeo lo ha introducido siguiendo las recomendaciones del GT29. Concretamente, el GT29 se inspiró en una guía de la Organización de Cooperación y Desarrollo Económico (OCDE) de 1980, en la que se hacía referencia a la *accountability* en el sentido de que «todo responsable de datos debería ser responsable de cumplir con las medidas que hagan efectivos los principios [materiales] expuestos» (GT29. WP173. p.7). Pues bien, como vemos se ponía el acento en el cumplimiento de 'medidas'. Aunque el fin último fuera cumplir con los principios de la guía, en la práctica, con lo que había que cumplir era con unas medidas concretas y efectivas para el cumplimiento de dichos principios.

Esto constituye la esencia del requisito de cumplimiento del principio de responsabilidad proactiva del RGPD. La prueba de esto es el desarrollo que se hace de la *accountability* en el art. 24 RGPD. En este artículo se insiste en que «el responsable del tratamiento aplicará

medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento» (art.24 RGPD). De este enunciado se extraen dos conclusiones.

En primer lugar, el principio de responsabilidad proactiva se proyecta en el cumplimiento de todo el RGPD, y no sólo en el de los principios enunciados en el art. 5.1 RGPD. Esto viene a reforzar lo ya explicado sobre la implicación de la *accountability*, en tanto que principio de derecho en la materia, en la interpretación y aplicación de todo el RGPD.

En segundo lugar, el objeto de cumplimiento es la adopción de medidas técnicas y organizativas concretas. Las cuales son configuradas en la norma como un instrumento para alcanzar el fin último, esto es, el mencionado cumplimiento de 'todo' el RGPD.

Por otro lado, llama la atención que el legislador europeo ha introducido el 'principio de proporcionalidad' en el artículo dedicado al responsable del tratamiento (art. 24 RGPD) que, a su vez, también desarrolla la *accountability*. Además, se establece que las políticas de protección de datos, cuando sean «proporcionadas» en relación con el tratamiento, se incluirán entre las medidas que debe aplicar el responsable del tratamiento (art. 24.2 RGPD).

Con ello, se introduce el conocido como triple juicio o «test de proporcionalidad» (PALMA, MURGA, 2018, p. 48). Esto significa que para la elección de las medidas se deberá realizar una ponderación aplicando el triple juicio de proporcionalidad. Así, se deberá valorar si la medida puede conseguir el objetivo esperado –juicio de idoneidad–, si no hay otra medida más moderada susceptible de conseguir el mismo resultado –juicio de necesidad– y si la medida es equilibrada en el sentido de que se derivan más beneficios que perjuicios –juicio de proporcionalidad en sentido estricto– (AEPD. 2018. Guía EIPD).

Por consiguiente, el principio de proporcionalidad debe guiar la elección de las medidas en aplicación de la *accountability* y, lo que es más relevante, además se proyecta en la aplicación de todo el RGPD, como una manifestación más de la responsabilidad proactiva. Esto es una consecuencia lógica de la propia naturaleza del derecho fundamental a la protección de datos que, como todo derecho, no es absoluto y debe ser ponderado conforme al principio de proporcionalidad (considerando 4 RGPD).

2.1.1.2. Requisito de ser capaz de demostrarlo: carga de la prueba

Como hemos indicado la *accountability* entraña una responsabilidad objetiva y no requiere de la intencionalidad en la acción del sujeto. Además, el legislador europeo ha querido reforzar el modelo de protección con la introducción de la inversión de la carga de la prueba. Con ello se introduce una presunción de incumplimiento, en el sentido de que corresponderá al responsable del tratamiento demostrar la conformidad con los requerimientos del RGPD (considerando 74 RGPD).

Adicionalmente, hemos dicho que la *accountability* es tanto directa como indirecta. Esto tiene como consecuencia que el responsable del tratamiento deberá demostrar no solo cuando el tratamiento se lleve a cabo por el mismo –responsabilidad directa–, sino también cuando sea realizado «por su cuenta» por un tercero –responsabilidad indirecta– (considerando 74RGPD).

En cuanto a qué es lo que debe demostrar, el requisito es doble. En primer lugar, es necesario acreditar que se ha cumplido con la *accountability*, mediante la adopción de las medidas técnicas y organizativas tendentes a garantizar todos los requerimientos del RGPD. Además, se requiere prueba de «la eficacia» de las mismas (considerando 74 RGPD), es decir, que las medidas son las adecuadas atendiendo a los riesgos y al ecosistema que rodea al tratamiento. Por tanto, «no incumplir ya no será suficiente» (RODRÍGUEZ, TRONCOSO, 2021, tomo I, p. 1330).

Por otro lado, «dichas medidas se revisarán y actualizarán cuando sea necesario» (art. 24.1 RGPD). De esta forma se introduce un requisito temporal, se debe poder demostrar 'en todo momento'. Además, se requiere la revisión de las medidas para su actualización en su caso. Esto hace referencia al ciclo de mejora continua del mundo de los estándares internacionales –normas ISO– y del *compliance,* en los cuales se ha inspirado el legislador europeo para la configuración del modelo de protección del RGPD (DURÁN, TRONCOSO, 2021, tomo I, p.1780).

Así, la auditoría en protección de datos es el instrumento adecuado para la revisión del cumplimiento de la *accountability*. Hay que tener en cuenta que las normas ISO incorporan ya auditorías en el proceso de certificación y en el ciclo de mejora continua –conocido como ciclo Deming–.Para demostrar el cumplimiento de la *accountability* contamos con las certificaciones, entre otras, con la ISO 27001:2013 para los Sistemas de Gestión de la

Seguridad de la Información –SGSI– y, más reciente y específica para la protección de datos personales, con la ISO 27701:2019 sobre Privacidad de la Información.

Asimismo, es importante mencionar otros dos instrumentos que sirven para demostrar el cumplimiento de la *accountability* , introducidos específicamente con esta finalidad en el art. 24.3 RGPD, los códigos de conducta y los mecanismos de certificación. La adhesión a cualquiera de ellos, como con la mayoría de medidas, crea una presunción de cumplimiento *iuris tantum,* es decir admite prueba en contra (Agencia Italiana de Protección de Datos. 2018. El Manual del DPD). Ambos cumplen la función de probar el cumplimiento y, a la vez, generan confianza (TRUJILLO, MURGA, 2018, p. 168).

Los códigos de conducta están regulados en los artículos 40 y 41 RGPD y art.38 LOPDGDD. En el RGPD no se incluye su definición. Podemos decir que los códigos de conducta son una suerte de guías de actuación para la práctica profesional para sectores concretos «asimilables a los códigos deontológicos o de buena práctica profesional» (SERRANO, TRONCOSO, 2021, tomo I, p. 2383). Lo relevante es que se introduce en el RGPD este instrumento, que proviene del mundo de la autorregulación, con carácter voluntario, pero una vez adheridos al mismo su cumplimiento es vinculante y sirve para demostrar el cumplimiento de la *accountability* y del RGPD.

Por otro lado, los mecanismos de certificados se encuentran regulados en los artículos 42 y 43 RGPD y art. 39 LOPDGDD. Tampoco contiene el RGPD su definición. La certificación «consiste en la obtención de un distintivo que acredita el cumplimiento» del RGPD (TRUJILLO, MURGA, 2018, p. 168). El RGPD hace referencia a «la creación de mecanismos de certificación, sellos o marcas de protección de datos a fin de demostrar el cumplimiento» del RGPD (art. 42.2 RGPD). La adhesión es voluntaria y no limitará la responsabilidad del responsable–o del encargado– del tratamiento por el incumplimiento del RGPD.

Por último, es necesario mencionar la importancia de ir recabando evidencias del correcto cumplimiento. En materia de prueba, el legislador europeo ha optado por introducir la libertad de forma. Muestra de ello es que se establece que hay que ser «capaz de demostrar» (art. 5.2 RGPD), sin especificar cómo hacerlo −el medio de prueba−. En materia de transparencia se establece que «la información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos» (art. 12.1 RGPD). Así, se dispone la libertad de elección en la forma de informar y, por tanto, también en la forma de dejar evidencia. Esta lógica puede

ser trasladada al resto de medidas de cumplimiento del RGPD. Sin embargo, debemos señalar que en determinadas ocasiones el RGPD requiere una forma concreta –la prueba escrita[23] u otra–. Esto es compatible con la libertad de forma como regla general.

En este sentido, conviene recordar que 'si bien la palabra es un contrato, presenta el problema de la prueba', lo cual puede ser trasladado a situaciones más allá de los contratos. Por esta razón, sea como fuere, hay que dejar evidencia de toda actuación o decisión que se adopte en cumplimiento de la *accountability*. Para esto, contamos con una herramienta infalible, la documentación. Así, se hace necesario y fundamental documentar correctamente cada una de las medidas que se apliquen en cumplimiento del principio de responsabilidad proactiva. Difícilmente podremos demostrar si antes no hemos guardado prueba documentada de todas y cada una de las decisiones adoptadas, incluida su motivación, esto es dejar la trazabilidad. Para esto, contamos con un recurso ideal, como son las normas UNE-ISO 30300 sobre gestión documental. La gestión de la documentación se torna así en un elemento de primer orden en cumplimiento de la *accountability*.

2.1.2. Medidas de cumplimiento

En este apartado abordamos las medidas técnicas y organizativas concretas en que se materializa el cumplimiento del principio de responsabilidad proactiva. Los mecanismos para la adecuada elección de dichas medidas serán analizados en el apartado dedicado a la seguridad enfocada en los riesgos.

Cumplir y demostrar –*accountability*– se traduce en la práctica en medidas concretas (TRONCOSO, 2021, tomo I, p. 905). El análisis de la conexión del considerando 74 y los artículos 5.2 y 24 del RGPD nos permitirá determinar cuáles son concretamente estas medidas.

En primer lugar, el RGPD establece que, en cumplimiento de su responsabilidad, el responsable del tratamiento está obligado a «aplicar medidas oportunas y eficaces y ha de poder demostrar …» (considerando 74 RGPD). Esta fórmula se repite varias veces a lo largo

[23] A título de ejemplo, se requiere la forma escrita para: el consentimiento (art. 7 RGPD), la información en materia de transparencia (art.12 RGPD), la designación del representante (art. 27 RGPD), el contrato de encargado (art.28 RGPD), el registro de actividades de tratamiento (art. 30 RGPD) y el asesoramiento de la autoridad de control al responsable tras la consulta previa (art. 36 RGPD).

del texto del RGPD. En ningún momento se especifica claramente cuáles son las medidas concretas que deben aplicarse en cumplimiento del principio de responsabilidad proactiva.

Seguidamente, el RGPD proclama de forma expresa el principio de responsabilidad proactiva mediante la fórmula «el responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo» (art. 5.2 RGPD). Una vez más, sin especificar las medidas –cómo cumplir y demostrar–. En este punto, traemos a colación las ya explicadas implicaciones de la *accountability* en la interpretación y aplicación de todo el RGPD. Con ello ponemos el acento en que todas las actuaciones que se realicen en cumplimiento del RGPD son medidas de cumplimiento del principio de responsabilidad proactiva.

Finalmente, el RGPD desarrolla el principio proclamado en su art. 5.2 en el capítulo IV dedicado al Responsable y encargado del tratamiento. En el primer artículo de este capítulo se establece que «el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento» (art. 24.1 RGPD). Tampoco señala cuáles son las medidas concretas. Sin embargo, sí introduce ciertos elementos que –como veremos en el apartado dedicado a la seguridad enfocada en los riesgos– hacen de indicadores para orientarnos en la elección de las medidas. Es importante reiterar que en este artículo se hace mención expresa a «las oportunas políticas de protección de datos» (art. 24.2 RGPD) como posibles medidas. Además, como ya hemos indicado, también se mencionan los códigos de conducta y los mecanismos de certificación como medidas adecuadas para demostrar la *accountability* (art.24.3 RGPD).

A lo largo del capítulo IV, el RGPD va desarrollando lo establecido en su art. 24. Así, se van introduciendo las medidas técnicas y organizativas en que se concreta el cumplimiento del principio de responsabilidad proactiva. Esto no debe llevarnos al error de pensar que las medidas en que se traduce la *accountability* son únicamente las incluidas en el mencionado capítulo IV, pues esto no es así. Todas y cada una de las medidas –disposiciones, decisiones u actuaciones– adoptadas en aplicación del RGPD constituyen medidas de cumplimiento del principio de responsabilidad proactiva. Esto es corolario de la proyección de la *accountability* en todo el RGPD, en tanto que principio general de derecho, en aplicación del art. 5.2 RGPD.

El GT29 propuso una lista de «medidas comunes de responsabilidad» para la aplicación de la *accountability* (GT29. WP173. p.12). Estas han sido recogidas por el RGPD, sin embargo, se trata de una lista abierta. El elemento que podría aglutinar todas estas medidas sería un

Programa de Cumplimiento de Protección de Datos Personales. A continuación, haremos una breve referencia a las medidas que deberían incluirse en este programa:

El análisis de riesgos (arts. 24 y 32 RGPD) es el punto de partida de toda actividad que implique el tratamiento de datos personales. La Agencia Española de Protección de Datos –AEPD–se refiere a él como «gestión de riesgos» (AEPD. 2018. Guía práctica de análisis de riesgos) y lo define como un «conjunto de actividades y tareas» destinadas a tomar el control de cualquier amenaza mediante una secuencia de acciones que incluyen tres fases, la identificación, la evaluación y el tratamiento de los riesgos con la aplicación de medidas. En el capítulo siguiente analizaremos con más profundidad en qué consiste esta herramienta y su importancia. Por ahora, es importante retener la idea de que el análisis de riesgos debe estar detrás, fundamentando la decisión, de todas las medidas técnicas y organizativas que se adopten en aplicación del principio de responsabilidad proactiva.

El registro de actividades de tratamiento –RAT– (art. 30 RGPD y 31 LOPDGDD) es el segundo elemento esencial. En el RGPD no se contiene la definición del RAT. Sobre la base de la definición de tratamiento contenida en el art. 4.2 del RGPD, esbozamos una definición del RAT de creación propia, como el documento escrito que ha de recoger fielmente el ecosistema que rodea a todos los tratamientos de datos personales, automatizados o no, realizados en una organización, recogiendo como mínimo punto por punto lo requerido en el art. 30 del RGPD. El RAT no sólo permite cumplir y demostrar, sino que además es una fuente de información inestimable para llevar a la práctica el resto de las medidas en aplicación de la *accountability*.

El Delegado de Protección de Datos (arts. 37 a 39 RGPD y arts.34 a 37 LOPDGDD) es otra pieza clave. En el RGPD no se contiene la definición del DPD. En el Considerando 97 del RGPD se hace referencia a «la persona con conocimientos especializados del Derecho y la práctica en materia de protección de datos» que ayuda, tanto a responsables como encargados, en la supervisión del cumplimiento del RGPD. Como veremos en el capítulo siguiente esta figura desempeña un rol esencial en el modelo de protección del RGPD. Si alguien puede ayudarnos a cumplir con el principio de responsabilidad proactiva, sin duda es el DPD.

Contar con procedimientos para atender el ejercicio de derechos en materia de protección de datos es también necesario. Los derechos de protección de datos han sido reforzados en el RGPD. Estos derechos son el derecho de transparencia e información (arts. 12-14 RGPD y art. 11 LOPDGDD), los derechos de acceso (art. 15 RGPD y art. 13 LOPDGDD), rectificación (art. 16

RGPD y art. 14 LOPDGDD) y supresión –olvido– (art. 17 RGPD y art. 15 LOPDGDD), el derecho a la limitación del tratamiento (art. 18 RGPD y art. 16 LOPDGDD), el derecho a la portabilidad (art. 20 RGPD y art. 17 LOPDGDD), el derecho de oposición (art. 21 RGPD y art. 18 LOPDGDD) y el derecho a no ser objeto de decisiones individuales automatizadas, incluida la elaboración de perfiles (art. 21 RGPD). Algunos de estos derechos ya existían, los conocidos como 'derechos ARCO'[24], el resto han sido creados. Si queremos cumplir con el principio de responsabilidad proactiva es necesario contar con protocolos para facilitar tanto la solicitud del ejercicio de derechos como su respuesta. Además, dentro de estos procedimientos se debe incluir la atención de quejas en materia de protección de datos (GT29. WP173. p.13).

Disponer de procedimientos de gestión de incidentes de seguridad -brechas- es fundamental. El concepto de brecha de seguridad es muy amplio. El RGPD se refiere a violación de la seguridad y lo define como «toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos» (art. 4.12 RGPD). No todo incidente puede ser calificado como brecha. La brecha de seguridad es un incidente de seguridad que afecta a los datos personales y puede generar consecuencias negativas para los derechos y libertades de los interesados (AEPD. 2018. Guía para la gestión y notificación de brechas de seguridad). Ante un supuesto de brecha se dispone tan sólo del plazo de 72 horas para notificar a la AEPD. Con la dificultad añadida de que, en este plazo, habrá que realizar un análisis de riesgos y recabar toda la información en torno a lo ocurrido, para decidir con conocimiento de causa sobre la adopción de medidas inmediatas para paliar o evitar sus efectos negativos y, a su vez, transmitir a la AEPD toda la información recabada. Por ello, la celeridad y eficiencia en la respuesta es vital. Esto hace necesario contar con un protocolo de actuación ante brecha de seguridad, para que, llegado el caso, sepamos actuar con rapidez y eficacia. Este protocolo debería formar parte del programa de proyección de la «cultura de la seguridad» (DAVARA, TRONCOSO, 2021, tomo I, p. 2136) de la organización y ser conocido por todos sus miembros.

La evaluación de impacto en la protección de datos –EIPD– es una medida muy relacionada con el análisis de riesgos. Podríamos decir que es una suerte de análisis de riesgos específico

[24] El concepto de derecho de cancelación ha sido reformulado, ahora es derecho de supresión.

y más profundo para una actividad de tratamiento concreta. Será objeto de análisis en el capítulo siguiente. En este apartamos nos limitamos a incidir en la idea de que forma parte de los elementos clave del nuevo modelo de protección del RGPD.

Las auditorías son también necesarias. El RGPD no las define, se refiere a ellas en el articulado en cuatro ocasiones: el encargado ha de permitir y contribuir a la realización de auditorías (art.28.3.h RGPD), entre las funciones del DPD está la supervisión de las auditorías (art. 39.1.b RGPD), las normas corporativas vinculantes incluirán auditorías (art. 47.2.j RGPD) y los poderes de investigación de las autoridades de control le facultan para realizar investigaciones en forma de auditorías (art. 58.1.b RGPD). De ello se infiere la obligatoriedad de la auditoría y que es una medida de la *accountability* –permite cumplir y demostrar–.

Las políticas de protección de datos personales (art. 24.2 RGPD) son el elemento aglutinador de todas las medidas. En el RGPD no se contiene una definición que nos permita delimitar sin ambages sus características y cómo y cuándo adoptar estas políticas. De la interpretación conjunta del considerando 78 y del art. 24 del RGPD se deduce que son introducidas como una obligación para el responsable del tratamiento. En el considerando 78, se indica que a fin de demostrar el cumplimiento del RGPD «el responsable del tratamiento debe adoptar políticas internas y aplicar medidas». En el art. 24.2 del RGPD se considera a estas políticas como una de las medidas de cumplimiento que se adoptaran cuando sean acordes con el ya mencionado test de proporcionalidad. Además, el RGPD define las normas corporativas vinculantes como políticas de protección de datos personales (art. 4.20 RGPD). Por tanto, podemos definir las políticas de protección de datos personales como el documento escrito, asumido por la alta Dirección de una organización, que recoge la asunción de responsabilidad y el compromiso de la organización con la protección de datos personales, así como los procedimientos para implementar correctamente las medidas en aplicación del RGPD. Por ello, todos los procedimientos y medidas que se mencionan a lo largo de este trabajo tendrían que estar recogidas en una política de protección de datos. Sin embargo, hay que tener en cuenta que, debido a las características de este trabajo, no mencionamos todas las posibles medidas.

2.2. Seguridad enfocada en los riesgos

En este apartado abordamos la seguridad enfocada en los riesgos como elemento integrante del modelo preventivo de la *accountability*. Para ello, realizamos una escueta aproximación al análisis de riesgos en sus diferentes manifestaciones en el articulado del Reglamento.

Como introducción interesa recordar lo que menciona la LOPDGDD en el apartado V de su preámbulo. Así, se hace hincapié en que el RGPD supone «la evolución de un modelo basado, fundamentalmente, en el control del cumplimiento a otro que descansa en el principio de responsabilidad activa, lo que exige una previa valoración por el responsable o por el encargado del tratamiento del riesgo que pudiera generar el tratamiento de los datos personales para, a partir de dicha valoración, adoptar las medidas que procedan». De esta forma se refiere al análisis de riesgos como requisito previo para la adopción de cualquier medida en cumplimiento del RGPD, cuya exigencia viene dada por la *accountability* –cumplir y demostrar–. Por tanto, el análisis de riesgos debidamente documentado es una herramienta para demostrar el cumplimiento normativo.

En el RGPD se hace referencia a los riesgos en muchas ocasiones. Dadas las características de este Trabajo, nos centraremos en el art. 24 dedicado a la Responsabilidad del responsable, en el art. 32 sobre Seguridad del tratamiento y en el art. 35 relativo a la Evaluación del impacto. En el apartado siguiente haremos también una breve alusión al análisis de riesgos previsto en el art. 25 sobre Protección desde el diseño y por defecto.

Del estudio del RGPD, de los artículos mencionados y de sus considerandos, podemos inferir que el legislador europeo ha introducido el análisis de riesgos en materia de protección de datos en dos niveles. Por un lado, se establece un análisis de riesgos digamos 'básico' como requisito previo a toda decisión sobre la adopción de medidas técnicas y organizativas (arts. 24, 25 y 32 del RGPD). Por otro lado, se regula la evaluación de impacto relativa a la protección de datos –EIPD–, conocida como PIA –*Privacy Impact Assessment*– en inglés, como una suerte de análisis de riesgos más 'exhaustivo' cuya realización no siempre es necesaria como veremos (arts. 35 y 25 RGPD). Además, es necesario reiterar que toda decisión sobre la implementación de medidas en cumplimiento de la *accountability* –no sólo en materia de seguridad– debe ir avalada por el oportuno análisis de riesgos previo, básico y/o EIPD. Esto es debido a la onda expansiva de la *accountability* en todo el RGPD –obligación de cumplir y demostrar–.

2.2.1. Análisis de riesgos

En cuanto a la definición de análisis de riesgos, el RGPD no la aporta. Atendiendo a la terminología de la ISO 27001; 2005, es la «utilización sistemática de la información disponible para identificar peligros y estimar riesgos» (DE LA PRADA, MURGA, 2018, p. 353). La AEPD se refiere a «gestión de riesgos» como «el conjunto de actividades y tareas» que, desarrolladas de forma ordenada y sistemática, hacen posible localizar, analizar y evaluar potenciales riesgos, con el fin de aplicar medidas para eliminarlos o mitigarlos (AEPD. 2018. Guía práctica de análisis de riesgos).

Es importante señalar que estamos ante un análisis de riesgos «de privacidad», esto es, de protección de datos personales (ACINAS, TRONCOSO, 2021, Tomo I, p. 2035). El RGPD se ha inspirado en el análisis de riesgos clásico centrado en las amenazas para las organizaciones, pero ha cambiado el foco del análisis y lo ha dirigido al interesado (PÉREZ, 2020, p.3).

En cuanto a su regulación en el RGPD, partimos de la idea de base antes mencionada de que el análisis de riesgos se requiere siempre que haya que decidir sobre la implementación de medidas técnicas y organizativas en aplicación del principio de responsabilidad proactiva. De esta idea se infiere que su regulación está implícita a lo largo del articulado del RGPD junto con la *accountability*. Por lo que se refiere a su regulación explícita, está contenida en los artículos 24, 25 y 32 y los considerandos 75 a 78 y 83 del RGPD.

En primer lugar, del art. 24 del RGPD se colige tanto que se deben implementar medidas técnicas y organizativas para asegurar, y demostrar, el cumplimiento del RGPD, como que dichas medidas deben basarse en los riesgos y ser proporcionadas (*ICO. Guide to the GDPR*). De igual forma, en el art. 25 se requiere el previo análisis de riesgos para la aplicación de medidas al objeto de implementar la privacidad desde el diseño y por defecto. Lo mismo ocurre con el art. 32 sobre medidas de seguridad, cuya decisión ha de ir precedida del análisis de riesgos oportuno.

La elección de la metodología para la realización del análisis de riesgos es libre. Existen muchas metodologías de análisis de riesgos para los sistemas de información que pueden utilizarse. Todas ellas comparten una serie de actividades que todo buen análisis de riesgos debe llevar a cabo. Esto es, el establecimiento del contexto, la identificación y valoración del impacto, la identificación de activos, la identificación de amenazas y vulnerabilidades, la evaluación de la

probabilidad de materialización de las amenazas, el cálculo de los riesgos potenciales, el tratamiento de los riesgos y la documentación del análisis de riesgos (PEREZ, 2020, p.4). Estos elementos mínimos se corresponden con las tres fases a que hace referencia la AEPD, es decir, la identificación de amenazas y riesgos, la evaluación de riesgos y el tratamiento de riesgos (AEPD. 2018. Guía práctica de análisis de riesgos).

No es posible en este Trabajo profundizar más. La idea que interesa retener es la de la relevancia del análisis de riesgos como medida de cumplimiento de la *accountability*.

2.2.2. Evaluación de impacto

La AEPD define la EIPD como «una herramienta con carácter preventivo» que hace posible «identificar, evaluar y gestionar» los posibles riesgos de los tratamientos de datos personales, con el fin de asegurar el respeto de los derechos y libertades de las personas físicas (AEPD. 2018. Guía EIPD). En la práctica la EIPD es una herramienta muy similar al análisis de riesgos, en el sentido de que ambas tienen como objetivo la identificación de riesgos, su posterior evaluación para determinar su nivel de gravedad y, en función del resultado, el tratamiento mediante la implementación de medidas de control que permitan su eliminación o reducción a niveles aceptables. En ambas, el fin último es proteger los derechos y libertades de los interesados en tanto que titulares de los datos personales.

La diferencia entre EIPD y análisis de riesgos se encuentra en el objeto y el nivel de exhaustividad del examen que se realiza. En cuanto al objeto, mientras que el análisis de riesgos es más genérico y se requiere como regla general con carácter previo a la adopción de cualquier medida en aplicación del RGPD, la EIPD está orientada a tratamientos concretos que entrañen alto riesgo. Respecto al nivel de exhaustividad, la EIPD requiere la conocida como «segunda vuelta» (PEREZ, 2020, p. 7). Es decir, una vez que se han implementado las medidas técnicas y organizativas correctoras para mitigar los riesgos, se calcula de nuevo el nivel de riesgo teniendo en cuenta estas medidas aplicadas. El resultado final debe arrojar un umbral de riesgo aceptable. Esta segunda vuelta no se requiere en el análisis de riesgos.

La EIPD se encuentra regulada en el art.35 y en los considerandos 75, 84 y 89 a 93 del RGPD. El prolijo art. 35 del RGPD regula sus caracteres esenciales: quién debe realizar la EIPD (apartado 1), cuándo es necesaria realizar la EIPD (apartados 1, 3 y 4), cuándo no se requiere (apartados 5 y 10), el mecanismo de coherencia con relación a la EIPD (apartado 6), el

contenido mínimo de la evaluación (apartado 7), el respeto de los códigos de conducta (apartado 8), la necesaria revisión de la EIPD tras cambios en los tratamientos (apartado 11) y la función de asesoramiento del DPD en la realización de la EIPD (apartado 2).

La evaluación de impacto debe ser realizada por el responsable del tratamiento, el RGPD es claro al respecto (DAVARA, 2018, p.1), así lo establece en el apartado 1 del art. 35. El legislador tiene en cuenta la carga que esto puede suponer para el responsable. Así, en el apartado 2, introduce al DPD como la figura que ha de asesorar al responsable en la realización de la EIPD. Para los supuestos en que no se cuente con un DPD por no entrar dentro de los supuestos de designación obligatoria, se puede recurrir a los servicios puntuales, mediante contratación, de un DPD para el desempeño de esta función de asesoramiento. Como veremos, contar con un DPD es altamente recomendable, incluso cuando no se esté obligado a ello.

En cuanto a cuándo debemos realizar la EIPD, en el RGPD se establecen dos vías. La primera vía se divide a su vez en otras dos, estos son los supuestos previstos en el art. 35 puntos 1 y 3. La segunda vía hace referencia a cuando concurren dos o más circunstancias de las previstas en la lista publicada por la AEPD en cumplimiento del art. 35.4 del RGPD.

Con referencia a la primera vía –art.35.3 RGPD–. A efectos prácticos, interesa verificar en primer lugar si concurre alguno de los tres supuestos previstos en el RGPD para la realización obligatoria de la EIPD: a) La toma de «decisiones que produzcan efectos jurídicos» o «afecten» de forma significativa a los interesados sobre la base de una «evaluación sistemática y exhaustiva de aspectos personales» de los mismos, como la «elaboración de perfiles»; b) Tratamientos «a gran escala» de datos personales relativos a «categorías especiales» o sobre «condenas e infracciones penales»; c) «Observación sistemática a gran escala» de zonas de «acceso público» (art. 35.3, letras a-b-c, RGPD). El legislador ha considerado la existencia de alto riesgo en estos casos, por ello los ha introducido en la norma.

En segundo lugar, hay que atender a la existencia de «alto riesgo», es decir, cuando sea 'probable' que un tratamiento «entrañe un alto riesgo» para los derechos y libertades de las personas físicas (art. 35.1 RGPD). La probabilidad viene dada por los elementos introducidos en el propio artículo para su apreciación, esto es, la naturaleza, alcance, contexto o fines del tratamiento, en especial si se utilizan nuevas tecnologías. De ello se infiere que se está pidiendo la realización de un análisis de riesgos de mínimos para valorar la existencia del alto riesgo. Esto es lo que la AEPD ha calificado como «analizar la necesidad de realizar una EIPD»

(AEPD. 2018. Guía EIPD). Por otro lado, la realización de la EIPD es obligada en los casos en que un análisis de riesgos previamente realizado arroje un resultado de 'alto riesgo'. A su vez, si tras realizada la EIPD, de esta se desprendiera 'alto riesgo' habría que consultar a la AEPD para que esta se pronuncie al respecto conforme a lo previsto en el art. 36 del RGPD.

Respecto a la metodología, la cual es de libre elección para los responsables del tratamiento (GT29. WP248), nos remitimos a lo explicado con relación al análisis de riesgos, pues es también aplicable a la EIPD. Ahora bien, sea cual sea la metodología elegida, el contenido mínimo requerido por el RGPD debe ser respetado, así como quedar correctamente documentada. La AEPD explica en una serie de etapas estos requisitos mínimos y añade otros que también estima necesarios (AEPD. 2018. Guía EIPD). Estos son: 1º Análisis preliminar, para evaluar la necesidad de realizar la EIPD, para la cual es necesario identificar las actividades de tratamiento y realizar un análisis de riesgos básico. 2º Análisis del contexto, en el que se incluye la descripción del ciclo de vida de los datos y el análisis de la necesidad y proporcionalidad del tratamiento. 3º Gestión de los riesgos, mediante la identificación de amenazas y riesgos, su evaluación y tratamiento. 4º. Informe de conclusiones, que incluya un 'plan de acción' con la asignación de responsabilidades para la implementación de las medidas y sus plazos, la justificación de la decisión de realizar o no la 'consulta a los interesados' con las opiniones de estos en su caso, así como, en su caso, la consulta a la AEPD conforme al art. 36 del RGPD. 5º Las decisiones y consideraciones del DPD.

Para terminar con este breve análisis de la EIPD, queremos resaltar su relevancia en el modelo de protección introducido por el RGPD. La EIPD es una herramienta que nos permite conocer con detalle el estado de cumplimiento del RGPD en la organización, sus fortalezas y sus debilidades, esto es el punto de partida para alinearse con los requerimientos del RGPD. Además, debemos disponer de esta información en todo momento y cada vez que se introduzcan cambios en los tratamientos tendremos que actualizar la EIPD para garantizar su validez (art.35.11 RGPD). En definitiva, la EIPD es una medida que nos permite cumplir y demostrar– *accountability*– y, además, contribuye a incrementar la cultura de protección de datos en las organizaciones.

2.3. Protección de datos desde el diseño y por defecto

En este apartado analizamos la protección de datos desde el diseño y por defecto como elemento fundamental en el modelo de protección introducido por el RGPD. Siguiendo la línea de este Trabajo, nos centraremos en lo esencial, esto es, su naturaleza y concepto, la conexión con el análisis de riesgos y con la *accountability*, su regulación, los sujetos obligados, las estrategias para su implementación, los requisitos de documentación y auditoría y la certificación.

En primer lugar, interesa aclarar que el legislador ha introducido dos 'principios' específicos en la materia en el artículo 25 del RGPD. Es cierto que ni la rúbrica de dicho artículo –protección de datos desde el diseño y por defecto– ni su ubicación[25] en el RGPD contribuyen para tal calificación. Lo lógico hubiera sido incorporar en la rúbrica de este artículo el término 'principios' y ubicarlos en el art. 5 dedicado a los principios. Sin embargo, de la interpretación hermenéutica del RGPD, incluso también de la literal, se desprende que estamos ante dos principios de protección de datos personales. Así lo demuestra el hecho de que se hace referencia a ellos en calidad de principios[26] en los considerandos 78 y 108 del RGPD[27]. Lo mismo ocurre en la guía sobre estos principios elaborada por el Comité Europeo de Protección de datos –CEPD–, conocido como –EDPB– por sus siglas en inglés. La consecuencia de esta calificación como principios es, como ocurre con la *accountability*, su proyección en la interpretación y aplicación de todo el RGPD.

Sobre la conexión tanto con el análisis de riesgos como con el principio de responsabilidad proactiva, hemos insistido a lo largo de este Trabajo en la idea clave de que toda decisión en aplicación del RGPD debe ir precedida por el oportuno análisis de riesgos. Esta regla básica cobra su mayor relevancia con relación a los principios del art. 25 del RGPD, pues precisamente su calificación como principios incrementa su importancia en el modelo de protección del RGPD, aunque, como veremos, con matices con relación a la privacidad por defecto. Por otro lado, la relación entre los principios del art. 25 del RGPD y el principio de responsabilidad proactiva es como la de 'dos vasos comunicantes', en el sentido de que las

[25] El art. 25 se encuentra en la Sección 1 sobre obligaciones generales del capítulo IV dedicado al Responsable del tratamiento y encargado del tratamiento.
[26] Véase los considerandos 78 y 108 RGPD. Se alude a los 'principios de protección desde el diseño y por defecto'.
[27] Véanse las pp. 4 y 7, entre otras, de la Guidelines 4/2019 on Article 25 Data Protection by Design and by Default.

características de todos ellos se traspasan de unos a otros, aumentando así la intensidad de la relación directa que tienen, aunque a primera vista no lo parezca. En efecto, difícilmente podremos cumplir con la *accountability* sin implementar los principios del art. 25. Dicho al revés, es imposible acatar los principios del art. 25 sin cumplir a la vez con la *accountability*, pues esta –recordemos– está detrás de cada decisión en aplicación del RGPD. Por ello, el GT29[28] propuso la introducción de estos principios juntos en la norma como refuerzo al marco regulatorio. Ahora bien, hay que tener presente que, en esta relación, la *accountability* está en un nivel jerárquico superior. Podemos decir, que los principios del art. 25 refuerzan el modelo de protección preventivo y, en especial, a su principio básico, la *accountability.*

El legislador ha introducido estos dos principios en el art. 25 en apartados separados. Esto no significa que actúen de forma independiente. Todo lo contrario, el *EDPB* ha aclarado que ambos principios deben ser considerados juntos para alcanzar el objetivo último que comparten, esto es, que el responsable del tratamiento aplique medidas efectivas para cumplir, y demostrar, los requerimientos del RGPD –*accountability*– (*EDPB. Guidelines on Article 25*). Los sujetos obligados son los responsables del tratamiento. Pero, la AEPD ha dejado claro que, si bien esto es así, hay otros actores[29] participantes en el tratamiento que deben tener en cuenta estos principios y la protección de datos personales en general, como son los proveedores y prestadores de servicios, desarrolladores de productos y aplicaciones o fabricantes de dispositivos (AEPD. Guía de Protección de Datos desde el Diseño). Los responsables, atendiendo a su deber de diligencia, deberán garantizar que dichos actores cumplen de forma efectiva con el RGPD. Además, conforme a la *accountability*, la aplicación de los principios del art. 25 se debe poder demostrar. Esto se traduce en una obligación de transparencia, en la obligación de justificar y documentar[30] y, además, todo ello ha de ser auditable (AEPD. Guía de Protección de Datos desde el Diseño). La certificación es una medida para demostrar el cumplimiento de la *accountability* y, también, de los principios del art. 25 del RGPD (art. 25.3 RGPD).

[28] Véase p. 2 del WP 168 -*The Future of Privacy-.*
[29] Esto se desprende del considerando 78 y del art. 28 del RGPD.
[30] Véase la Guidance on Article 25 of the Regulation 2018/1725 and internal rules restricting data subjects rights, del Supervisor Europeo de Protección de Datos. Se abordan aspectos sobre la documentación.

2.3.1. Privacidad desde el diseño

El principio de privacidad desde el diseño –PbD– está regulado en el art. 25.1 y en el considerando 78 del RGPD[31]. Basaremos nuestro análisis en la guía para la implementación del PbD de la AEPD (AEPD. Guía de Protección de Datos desde el Diseño).

El concepto de PbD hace referencia a la necesidad de incorporar los requisitos de privacidad desde las primeras fases del diseño de todo proyecto, producto o servicio que conlleve el tratamiento de datos personales. La PbD implica utilizar un enfoque orientado a la gestión de los riesgos, como un planteamiento dinámico y de mejora continua, capaz prevenir o mitigar los potenciales «riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas», mediante la aplicación de «medidas técnicas y organizativas» conforme al art. 32 del RGPD. La PbD implica para el responsable, obligado por la *accountability*, una actitud crítica de su propia actuación, en todo momento y que deje prueba del cumplimiento del RGPD. Por otro lado, los términos 'protección de datos desde el diseño' y 'privacidad desde el diseño' son sinónimos, el primero es una evolución del segundo.

La implementación de la PbD consiste en la aplicación de medidas orientadas a la construcción de la privacidad como un modo de actuación predeterminado. En la práctica esto puede logarse aplicando los Siete Principios Fundacionales definidos por la ideóloga de la PbD, Ann Cavoukian. Dada su importancia, hacemos una somera explicación de estos principios (AEPD. Guía de Protección de Datos desde el Diseño):

1. «Proactivo, no reactivo; preventivo, no correctivo». Consiste en anticiparse a los eventos que afectan a la privacidad antes de que sucedan, pues la PbD 'huye de la política de subsanar'.

2. «La privacidad como configuración predeterminada». Trata de que la configuración por defecto quede establecida desde el diseño de la forma más respetuosa posible con la privacidad, se fundamenta en el principio de minimización.

3. «Privacidad incorporada a la fase de diseño». La privacidad no es una capa adicional, al contrario, está integrada de forma indisoluble en los sistemas, aplicaciones, productos, servicios y prácticas de negocio y procesos de la organización.

[31] Véase art. 25.1 y considerando 78 del RGPD.

4. «Funcionalidad total, pensamiento “todos ganan”», 'win win' o 'suma cero'. La PbD rompe con la tradicional idea de que se gana privacidad a costa de perder otras funcionalidades, como beneficio empresarial, funcionalidad o seguridad.

5. «Aseguramiento de la privacidad en todo el ciclo de vida», 'end to end'. La privacidad nace en el diseño, antes de que el sistema esté en funcionamiento, y debe garantizarse durante todo el ciclo de vida de los datos.

6. «Visibilidad y transparencia». La transparencia es el pilar para poder demostrar la diligencia y la *accountability*. Las políticas de protección de datos deben ser claras, concisas e inteligibles.

7. «Enfoque centrado en el usuario» . Puesto que el fin último es garantizar los derechos y libertades de los interesados, cualquier medida debe ir dirigida a alcanzar este fin.

Sobre las medidas en que se concretan estos principios, el RGPD nombra dos ejemplos en el art. 25.1, la seudominización y la minimización. La AEPD incluye en su guía: 1. Minimización, recoger y tratar la mínima cantidad de datos posible. 2. Ocultación, limitar la exposición de los datos, garantizando la confidencialidad y desvinculación. 3. Separación, para evitar el perfilado mediante el uso de datos personales de un mismo sujeto, en una misma entidad y desde tratamientos independientes. 4. Abstracción, limitar al máximo el detalle de los datos. 5. Información, asegurar que los interesados estén bien informados. 6. Control, garantizar que el interesado decida sobre sus datos personales durante todo el ciclo de vida del dato. 7. Cumplimiento, garantizar el respeto del RGPD, de la LOPDGDD y de la normativa sectorial en la materia. 8. Demostración, establecer procedimientos que permitan recoger evidencias de cara al cumplimiento de la *accountability* (AEPD. Guía de Protección de Datos desde el Diseño).

Por último, haremos una breve referencia al aspecto temporal y a otros elementos que deben ser tenidos en cuenta, junto con el análisis de riesgos, para la correcta implementación de las medidas en aplicación del PbD. Estos elementos son el estado de la técnica, el coste de aplicación y la naturaleza, ámbito, contexto y fines del tratamiento. Todos ellos deberán ser considerados por el responsable del tratamiento. Sobre al aspecto temporal, la PbD debe ser implementada tanto en el momento de determinar los medios del tratamiento −en la fase de diseño− como durante el propio tratamiento. Con ello, se pretende una protección real y efectiva y, dado que los tratamientos pueden cambiar, las medidas deberán adaptarse a tales cambios, incluso modificando el diseño si fuera necesario.

2.3.2. Privacidad por defecto

El principio protección por defecto -PDpD- está regulado en el art. 25.2 y considerando 78 del RGPD[32]. Como con la PbD, basaremos nuestro análisis en la guía para la implementación del PDpD de la AEPD (AEPD. Guía de Protección de Datos por Defecto).

El concepto de PDpD podemos extraerlo del propio RGPD, concretamente, cuando establece que, «por defecto», solo deberán ser tratados los datos personales que sean «necesarios» para cada finalidad específica del tratamiento (art. 25.2 RGPD). Con ello, se hace una referencia directa al principio de minimización del RGPD, es decir, a que sólo deben ser objeto de tratamiento los datos personales que sean «adecuados, pertinentes y limitados a lo necesarios en relación con los fines» (art. 5.1.c RGPD).

El objetivo último de la PDpD es la configuración 'por defecto', es decir, sin la intervención de los interesados –las personas físicas cuyos datos personales se trata de garantizar con la PDpD–. De este modo, se persigue que los tratamientos nazcan ya de la forma más respetuosa posible con los principios de protección de datos, se apuesta por un procesamiento mínimamente intrusivo. Los elementos que deben tenerse en cuenta en la configuración por defecto están recogidos en el propio art. 25.2 del RGPD. Estos elementos conectan con los principios del tratamiento del art.5 del RGPD. Así, en el PDpD se concretan y materializan estos principios del art. 5, para que la configuración de los sistemas y proyectos a los que se aplica, como medida preventiva, cumplan con la *accountability* y con el RGPD.

Enumeramos brevemente los mencionados elementos y su conexión con los principios del tratamiento: 1. Mínima cantidad de datos personales, es decir, 'principio de minimización' (art. 5.1.c). 2. Mínima extensión del tratamiento, esto es, 'principio de limitación de la finalidad' (art. 5.1.b). 3. Mínimo plazo de conservación, o, 'principio de limitación del plazo de conservación' (art.5.1.e). 4. Mínima accesibilidad a los datos personales, es el 'principio de integridad y confidencialidad' (art. 5.1.f) (MIRALLES, TRONCOSO, 2021, tomo I, p. 1818).

Con referencia al principio de integridad y confidencialidad. A rasgos generales, la 'integridad' persigue mantener con exactitud la información tal cual fue generada, sin que sea manipulada o alterada por personas o procesos no autorizados. A su vez, la 'confidencialidad' consiste en

[32] Véase art. 25.2 en relación con el considerando 78 del RGPD.

asegurar el acceso a la información únicamente a las personas autorizadas. El RGPD, primero se refiere a la 'mínima accesibilidad'. En la línea siguiente introduce una reiteración, establece que las medidas en aplicación de la PDpD «garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas» (art. 25.2 RGPD). Con ello, se insiste en el requerimiento de que el tratamiento nazca ya con una configuración que garantice la integridad y confidencialidad, sin necesidad de la intervención del interesado. En definitiva, se apuesta por la conocida 'política de mínimos privilegios'.

Introducimos un matiz con relación al análisis de riesgos. Este constituye un requisito previo para la adopción de toda medida en aplicación del RGPD, incluidas las relativas a los principios del art.25 del RGPD. Sin embargo, respecto al PDpD, las medidas para su implementación no estarán condicionadas por el análisis de riesgos, pues estas se adoptarán 'por defecto', como medida preventiva y en todo caso, independientemente del resultado de este (AEPD. Guía de Protección de Datos por Defecto). Sobre el elemento temporal, la PDpD ha de implementarse antes del tratamiento, para que por defecto las medidas formen parte del sistema de protección.

En cuanto a las posibles estrategias que permiten implementar la privacidad por defecto, tenemos: 1. Recogida de datos, se deben analizar los tipos de datos que se recaban con el criterio de minimización indicado, en función de los productos y servicios seleccionados por el interesado. 2. Tratamiento de los datos, se analizarán los procesos asociados a dichos tratamientos para que se acceda a los mínimos datos personales necesarios para el tratamiento. 3. Conservación, se implementará una política de conservación de datos personales que permita, con un criterio restrictivo, eliminar los datos personales que no sean estrictamente necesarios. 4. Accesibilidad, se debe limitar el acceso a los datos personales de terceros no autorizados.

2.4. Delegado de Protección de Datos

Este último apartado lo dedicamos al análisis del Delegado de Protección de Datos, una figura clave en el modelo de protección del RGPD sustentado en la *accountability*. Abordaremos con brevedad su rol, posición y funciones y aspectos relacionados con su designación.

El DPD se encuentra regulado en los arts. 37 a 39 y considerado 97 del RGPD y en los arts. 34 a 37 de LOPDGDD. Ninguna de estas dos normas aporta la definición del DPD. Del análisis de la regulación de la figura podemos inferir que es «la persona con conocimientos especializados del Derecho y la práctica en materia de protección de datos» (considerando 97 RGPD), que desempeña la tarea de ayudar, tanto a responsables como encargados del tratamiento, en la supervisión dentro de la organización del cumplimiento de la normativa de protección de datos personales, con independencia, dotado de medios adecuados para ello y desde una posición al más alto nivel dentro de la organización.

La figura del DPD no es nueva. Su origen lo encontramos en Alemania en 1977, en su Ley Federal de Protección de Datos. La Directiva 95/46/CE ya lo regulaba, aunque no era obligatorio, los Estados miembros –EM– podían elegir, en España se optó por no incorporarlo. El antecedente más reciente lo tenemos en el Reglamento (CE) n.º 45/2001[33] para el tratamiento de datos personales por las instituciones y los organismos de UE, ya derogado.

El legislador europeo, atendiendo a las recomendaciones del GT29 y a la previa experiencia positiva de esta figura en otros países, ha apostado por apuntalar su modelo de protección con la introducción del DPD. Por ello, refuerza la figura configurándola como «una institución crucial nueva que debe considerarse como un medio esencial para dar efecto práctico» (T4DATA. 2019) a la *accountability*. Para potenciar esta institución, se otorga una presunción de cumplimiento a las «indicaciones proporcionadas» por el DPD (considerando 77 RGPD). Con ello, se pretende incentivar a las organizaciones al recurso del DPD pues esto redundará en un mejor cumplimiento del RGPD. Como veremos, el rol desempeñado por el DPD es crucial en el modelo de protección preventivo del RGPD fundamentado en la *accountability*.

[33]Derogado por el vigente Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE.

2.4.1. Rol, posición y funciones

Introducimos este apartado con una cita de la AEPD sobre el rol del DPD que parece evocar al 'garante de la legalidad', «esta figura constituye uno de los elementos claves del RGPD y un garante del cumplimiento de la normativa de protección de datos en las organizaciones» (AEPD. Blog). Para el desempeño de este significativo papel, se atribuyen al DPD importantes funciones y, para garantizar que pueda desempeñarlas correctamente, se le dota de independencia y de una posición destacada y visibilidad dentro de la organización. Basaremos nuestro análisis en lo establecido en el RGPD, en la LOPDGDD, en las directrices del GT29 sobre el DPD –WP243– y en el esquema de certificación y directrices sobre el DPD en las Administraciones públicas de la AEPD.

Las funciones del DPD están reguladas en el art. 39 y en el considerando 97 del RGPD. La LOPDGDD complementa esta regulación básica en su art. 37. El RGPD establece las siguientes funciones mínimas del DPD (art. 39.1 RGPD): 1. «Informar y asesorar» a responsables y encargados del tratamiento y a los empleados de sus obligaciones conforme a toda la normativa de protección de datos, es decir, el RGPD, la normativa nacional y de la UE. 2. «Supervisar el cumplimiento» de dicha normativa y de las políticas de protección de datos de los responsables y encargados, en especial la asignación de responsabilidades, la concienciación y la formación del personal y las auditorías. 3. «El asesoramiento» acerca de la EIPD, cuando se le solicite, así como supervisar la correcta aplicación del art. 35 del RGPD. 4. «Cooperar con la autoridad de control», en España la AEPD. 5. «Actuar como punto de contacto» con la autoridad de control en todas las cuestiones relacionadas con la protección de datos, como la consulta previa del art. 36 del RGPD, incluidas las consultas sobre otros asuntos.

La LOPDGDD atribuye al DPD otras funciones complementarias en su art. 37 dedicado a las reclamaciones de los afectados. La AEPD proporciona una lista de funciones genéricas del DPD, las cuales se concretan en tareas de «asesoramiento y supervisión» (AEPD. Esquema de certificación). Además, el RGPD regula una suerte de 'cajón de sastre' que da cabida para que el DPD pueda «desempeñar otras funciones y cometidos», siempre que estas «no den lugar a conflicto de intereses» (art.38.6 RGPD). Destaca que se opte por introducir esta previsión en el artículo dedicado a la posición del DPD, y no en el de sus funciones.

Para el desempeño de estas funciones, el DPD asume un 'papel de facilitador' en relación con la AEPD. Su actuación podría llegar a evitar la posible sanción de la AEPD, por tanto, estamos ante una suerte de 'actuación de conciliación del DPD'. Además, cuando aprecie una vulneración relevante de la norma, está obligado a documentarlo y a comunicarlo a la dirección de la organización (art. 36.4 LOPDGDD).

Por otro lado, el enfoque en los riesgos también está presente en la regulación de esta figura. El DPD tiene un deber de diligencia en el desempeño de sus funciones que le obliga a prestar «la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento» (art. 39.2 RGPD).

Con relación a la responsabilidad del DPD por el desempeño de sus funciones, si este actuara apartado de los criterios legales que establece el RGPD podría incurrir en responsabilidad civil, penal o profesional, en su caso. Quien asume la responsabilidad por los daños y perjuicios ocasionados por el tratamiento es el responsable o, en su caso, el encargado del tratamiento (art. 82 y 24 RGPD). Pero, estos podrían «dirigir la acción de repetición contra» el DPD (TOMÁS, MURGA, p. 185) para reclamarle en vía civil la cuantía que proceda.

En cuanto a la posición del DPD, se encuentra regulada en el art. 38 del RGPD y en el art. 36 de la LOPDGDD y viene a garantizar que este pueda desempeñar sus amplias funciones. A continuación, enumeramos los caracteres más significativos:

El responsable y el encargado del tratamiento garantizarán que el DPD «participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos» (art. 38.1 RGPD), para ello, estos potenciarán la visibilidad del DPD dentro de la organización. Además, le respaldarán «facilitando los recursos necesarios para el desempeño de sus funciones y el acceso a los datos personales y las operaciones de tratamiento, y para el mantenimiento de sus conocimientos especializados» (art. 38.2 RGPD). En especial, garantizarán la independencia del DPD, es decir, «que no reciba ninguna instrucción en lo que respecta el desempeño de sus funciones» (art. 38.3 RGPD), por ello, este no será instruido sobre cómo abordar los asuntos o para que adopte una decisión en concreto.

Así, el DPD «no será destituido ni sancionado por desempeñar sus funciones, salvo que incurriera en dolo o negligencia grave» (art. 36.2 LOPDGDD). Se consideran sanciones las siguientes: falta de ascensos o su dilación, el impedimento a la formación profesional o la

denegación de otras prestaciones que otros empleados reciben. Tampoco podrá ser objeto de amenazas de sanciones, aunque no lleguen a materializarse. El DPD «rendirá cuentas directamente al más alto nivel jerárquico» (art. 38.3 RGPD) y podrá expresar sus discrepancias cuando la organización vaya en contra de la norma (GT29. WP243).

El DPD estará sujeto al «deber de confidencialidad y secreto» (art.36.3 LOPDGDD) «en lo que respecta al desempeño de sus funciones» (art. 38.5 RGPD). Además, tendrá «acceso a los datos personales y procesos de tratamiento» para el ejercicio de sus funciones, la organización no podrá oponerse a ello so pretexto del deber de confidencialidad o secreto.

El responsable o encargado del tratamiento garantizará que las funciones y cometidos del DPD no den lugar a «conflicto de intereses» (art. 38.6 RGPD y art.36.2 LOPDGDD). Para ello, se debe garantizar que el DPD cuente con total independencia y autonomía en su actuación. Los puestos dentro de la organización que, como norma general, pueden generar conflicto de intereses son los siguientes: los puestos de Alta Dirección; otros cargos inferiores en la estructura organizativa que impliquen determinar los fines y medios del tratamiento de datos personales; en el supuesto de que el DPD sea un abogado en ejercicio, no podrá representar a la organización responsable ni al encargado ante los tribunales en casos relacionados con la protección de datos (GT29. WP243).

El GT29 recomienda una serie de medidas para evitar el conflicto de intereses: determinar los posibles puestos incompatibles con la función de DPD; elaborar normas internas destinadas a evitar conflictos de intereses; incluir una explicación general sobre los conflictos de intereses; declarar que el DPD no incurre en ningún conflicto de intereses respecto a sus funciones, esto es una forma de concienciar sobre este requisito; incluir otras salvaguardias en las normas internas de la organización (GT29. WP243).

2.4.2. Designación

Los supuestos en que es obligatorio designar al DPD vienen determinados por el RGPD y la LOPDGDD. El art. 37.1 del RGPD establece tres supuestos para su designación obligatoria: 1. Tratamiento realizado por «autoridad u organismo público». 2. Tratamientos relacionados con las «actividades principales» de responsables o encargados, que según «su naturaleza, alcance y/o fines» realicen una «observación habitual y sistemática» de interesados «a gran escala». 3. Tratamientos «a gran escala de categorías especiales de datos y «datos relativos a condenas

e infracciones penales», relacionados con las «actividades principales» de responsables o encargados. El GT29 ha explicado ciertos conceptos contenidos en este artículo, como gran escala, establecimiento principal u observación habitual y sistemática, cuyo entendimiento es necesario para la correcta aplicación de este artículo (WP243). A su vez, el art. 34.1 de la LOPDGDD[34] complementa lo anterior mediante la introducción de una lista abierta de supuestos de designación obligatoria del DPD.

La designación voluntaria del DPD está prevista en la norma. El RGPD regula la posibilidad de «nombrar un único» DPD para el «grupo empresarial», a condición de que el acceso al mismo resulte fácil desde cualquier establecimiento (art. 37.2 RGPD). La accesibilidad efectiva al DPD, así como su ubicación en la UE –como regla general salvo excepciones puntuales–, son necesarias para que este pueda desempeñar sus funciones (GT29. WP243). En cuanto a las Administraciones Públicas, podrán optar por «designar un único» DPD, en función de «su estructura organizativa y tamaño» (art.37.3 RGPD). La LOPDGDD regula la posibilidad de designación voluntaria del DPD en el art. 34.2, en cuyo caso quedará sometido al régimen previsto para los supuestos de designación obligatoria.

En cualquier caso, la designación del DPD es siempre recomendable, sea de forma obligatoria o voluntaria. Llegado el caso, ante un posible expediente sancionador, la AEPD podría considerar como una atenuante contar con un DPD de forma voluntaria y, como una agravante, no haberlo designado cuando es preceptivo. Además, a esto se añade que esta figura es la llamada a facilitar la compresión de la extensa normativa en la materia. Sin olvidar que constituye una medida que permite cumplir y poder demostrar –*accountability*–.

El DPD puede ser una persona física o jurídica, interna o externa, ambas posibilidades están prevista en la norma. En efecto, el DPD podrá «formar parte de la plantilla» de la organización o «desempeñar sus funciones en el marco de un contrato de servicios» (art. 37.6 RGPD), es decir, DPD interno o externo respectivamente. En cuanto al DPD interno, corresponderá al responsable y al encargado del tratamiento analizar si entre las personas de la plantilla de la organización hay alguien que cumpla con los requisitos exigidos por el RGPD y la LOPDGDD para poder ser designado. Si se diera el caso, el nombramiento a nivel interno del DPD se

[34] Véase art. 34.1 LOPDGDD.

podría realizar mediante la inclusión de una cláusula específica a tal efecto en el contrato laboral de la persona o personas designadas.

Respecto al DPD externo, es necesario plasmar en un contrato su nombramiento, cuyo contenido debe contemplar todos los extremos exigidos por la norma, incluida una cláusula relativa a la protección de datos con 'algunos' extremos del art. 28 del RGPD relativo al contrato de encargado. Ahora bien, decimos 'algunos' pues el DPD no es un encargado del tratamiento, su independencia es incompatible con su instrucción en el ejercicio de sus funciones, este extremo debería incluirse en la mencionada cláusula y garantizarse de forma efectiva. En todo caso, la designación, nombramiento y cese del DPD, obligatorio o voluntario deberá ser comunicado a la AEPD en el plazo de diez días (art. 34.2 LOPDGDD). A su vez, la AEPD y las autoridades autonómicas de protección de datos «mantendrán una lista actualizada» de los DPD, «accesible por medios electrónicos» (art. 34.4 LOPDGDD).

En lo referente a la dedicación, el DPD desempeñará sus funciones a tiempo completo o parcial (art. 34.5 LOPDGDD). Para decidir sobre ello, los responsables y encargados del tratamiento tendrán en cuenta las circunstancias del tratamiento, como su volumen, la naturaleza de los datos, categorías especiales u otras y los riesgos, entre otras. En todo caso, garantizarán que el DPD disponga del tiempo necesario para el desempeño correcto de sus funciones y que no se dé el mencionado conflicto de intereses.

Acabamos con una sucinta referencia a la cualificación profesional del DPD. El RGPD establece que el DPD será «designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones indicadas en el artículo 39» (art. 37.5 RGPD). Es decir, no se requiere ser diplomado o licenciado en Derecho, pero sí tener conocimientos de la normativa de protección de datos. Esto es complementado por la LOPDGDD, cuando establece que los requisitos requeridos para ser designado DPD podrán «demostrarse, entre otros medios, a través de mecanismos voluntarios de certificación que tendrán particularmente en cuenta la obtención de una titulación universitaria que acredite conocimientos especializados en el derecho y la práctica en materia de protección de datos» (art. 35 LOPDGDD). Así, para la certificación, que es 'voluntaria', se tendrán en cuentan titulaciones universitarias especializadas, como un máster en protección de datos personales, pero no es así para el ejercicio profesional como DPD, la diferencia es importante.

3. Conclusiones

En este TFM se ha abordado el análisis jurídico del principio de responsabilidad proactiva o *accountability,* con la pretensión de facilitar su compresión, especialmente su significado y alcance así como las obligaciones que genera, al objeto de resolver el problema planteado, concretamente la dificultad de entender este concepto y así reducir la inseguridad jurídica.

A nuestro juicio, esta dificultad deriva del hecho de que estamos ante un principio de derecho, que es por esencia vago e impreciso, es decir, un concepto jurídico indeterminado, lo cual dificulta su interpretación. Si a esto le sumamos que la *accountability* se proyecta en todo el RGPD, su entendimiento se hace aún más necesario.

Tras realizar este trabajo llegamos a las siguientes conclusiones:

PRIMERA.– La entrada en vigor del RGPD ha marcado un hito en la regulación en materia de protección de datos personales, supone un antes y un después. Esto es debido al cambio radical que supone la introducción del nuevo modelo de protección de datos basado en la prevención y sustentado por el principio de responsabilidad proactiva.

Este sistema preventivo es configurado en torno a una serie de elementos, interconectados y acoplados tanto al modelo como entre sí, cuya actuación conjunta y coordinada es necesaria para su correcto funcionamiento. A nuestro juicio los componentes esenciales de este sistema son un nuevo enfoque de la seguridad basada en los riesgos, los principios de protección desde el diseño y por defecto, el Delegado de Protección de Datos y el principio de responsabilidad proactiva o *accountability*.

Estamos por tanto ante un sistema complejo, donde diferentes elementos, principios de derecho y requisitos normativos, confluyen a lo largo del texto del RGPD. Esto, a nuestro parecer dificulta su entendimiento y a la postre puede redundar en su peor aplicabilidad.

SEGUNDA.– El principio de responsabilidad proactiva es la base que sustenta este modelo preventivo. Sin la *accountability* el engranaje de este sistema no puede funcionar.

Consideramos que su incorporación en el RGPD obedece al recurso a la técnica legislativa consistente en introducir 'principios de derecho', en la búsqueda de la flexibilidad que los caracteriza. Esto permitirá al RGPD tanto adaptarse mejor al caso concreto como que no quede obsoleto en poco tiempo debido a la gran velocidad en la que se producen los cambios sociales en un mundo interconectado con avances tecnológicos constantes.

Así, a nuestro juicio, nos encontramos con la paradoja de que el elemento clave para la correcta interpretación y aplicación del RGPD es un concepto jurídico indeterminado. Consideramos que esto genera inseguridad jurídica.

TERCERA.– A nuestro parecer, el alcance de la *accountability* es enorme. Su naturaleza de principio de derecho, con sus rasgos de vaguedad e indeterminación, potencia su importancia. Consideramos que la *accountability:*

Debe guiar la actuación de responsables y encargados del tratamiento, la cual debe estar motivada por el cumplimiento de la norma y la capacidad de poder demostrarlo. Así, marca dos límites infranqueables para que esta actuación sea aceptable, el cumplimiento y la prueba.

Por otro lado, establece unas directrices de actuación graduables en función del caso concreto. Además, opera a un nivel jerárquico superior al resto de principios del RGPD.

Finalmente, es reseñable su función informadora. La *accountability* debe inspirar, orientar o informar todo el RGPD y el resto de normativa en la materia. Pensamos que esto es debido al efecto expansivo que produce la aplicabilidad directa de la figura del Reglamento de la UE.

CUARTA.–. En cuanto a su significado, el concepto de *accountability* está compuesto por sus dos requisitos, el de cumplir y ser capaz de demostrarlo.

A nuestro juicio, esto hace referencia a lo que en derecho español se conoce como responsabilidad objetiva, directa o indirecta. Es responsabilidad objetiva o por resultado, pues es ajena a la intencionalidad de la acción del sujeto causante. Se responde como responsable por el incumplimiento o por la imposibilidad de poder demostrar la actuación acorde a la norma, independientemente de que se haya querido o no este resultado. Además, es directa, ya que son los propios actos contrarios a la norma del responsable los que generan su

responsabilidad. Por último, es indirecta, ya que el responsable podría responder por los actos de un tercero, como es el encargado del tratamiento.

Consideramos que el requisito de cumplir hace referencia a todo el RGPD y al resto de la normativa en la materia –no sólo a los principios del tratamiento–. La interpretación de los diferentes factores analizados nos lleva a esta conclusión, entre ellos, la combinación de los arts. 5 y 24 del RGPD, la naturaleza de principio de derecho de la *accountability,* la expansión que genera la figura del Reglamento y los documentos del GT29. Además, el objeto del cumplimiento es la adopción de medidas concretas, técnicas y organizativas, las cuales se decidirán atendiendo al principio de proporcionalidad. A nuestro juicio esto es muy importante, pues una medida desproporcionada constituye por sí misma un incumplimiento.

Pensamos que el requisito de ser capaz de demostrar constituye el verdadero revulsivo del modelo del RGPD, puesto que una medida ineficaz supone el incumplimiento del RGPD. En efecto, hay que demostrar que se han adoptado las medidas técnicas y organizativas tendentes a garantizar el respeto de la norma y, además, que éstas son realmente efectivas. Consideramos que con esto se ha introducido una presunción de incumplimiento y la inversión en la carga de la prueba. Con ello, de forma indirecta se ha introducido en el RGPD una obligación de gestión correcta de la documentación como medio de prueba.

QUINTA.– Las obligaciones que genera la *accountability* consisten en la implementación de medidas concretas para cumplir y demostrar. A nuestro parecer, todas y cada una de las medidas adoptadas –sean estas disposiciones, decisiones u acciones– en cumplimiento del RGPD son medidas de cumplimiento de la *accountability*.

Pensamos que un Programa de Cumplimiento de Protección de Datos Personales podría aglutinar todas las medidas requeridas por el RGPD. Este, como mínimo, debería contar con procedimientos para realizar análisis de riesgos y EIPD, el RAT, el DPD, procedimientos para el ejercicio de derechos en la materia, protocolo de brechas, auditorías y políticas de protección de datos personales.

SEXTA.–. Con relación a los elementos esenciales que integran el modelo preventivo junto con la accountability :

Sobre la seguridad enfocada en los riesgos. Consideramos que se introduce el análisis de riesgos de protección de datos como medida trasversal de cumplimiento de la *accountability*. Se requiere siempre que haya que decidir sobre medidas en aplicación del RGPD. A nuestro entender, el análisis de riesgos se proyecta en todo el RGPD junto la *accountability* en dos niveles. A nivel básico, tenemos el análisis de riesgos regulado en los arts. 24, 25 y 32 del RGPD, que debe realizarse de forma general como requisito previo para decidir sobre la adopción de medidas. A un nivel más profundo, como análisis exhaustivo, está la EIPD del art. 35 del RGPD, necesaria sólo cuando se dé alto riesgo o así lo exija la norma.

Con relación a la protección desde el diseño y por defecto como medida preventiva de cumplimiento de la *accountability.* Estimamos que se trata de dos principios, aunque no se mencione en la rúbrica del art. 25 del RGPD, que operan de forma conjunta −no de forma independiente−. La PbD implica que la protección de datos se tenga en cuenta desde las primeras fases del diseño de todo proyecto, producto o servicio que entrañe tratamiento de datos personales. La PDpD supone que la configuración por defecto −sin intervención humana− sea lo más respetuosa posible con la protección de datos de las personas físicas.

En cuanto al Delegado de Protección de Datos. Pensamos que es una figura indispensable en este modelo de protección y que los objetivos de la *accountability* no se pueden alcanzar sin él. Creemos que por ello se le han atribuido las importantes funciones de asesoramiento y consulta y se le ha dotado de una posición destacada en la organización, de independencia y de visibilidad.

SÉPTIMA.– Para terminar, esbozamos una definición de la *accountability* de creación propia, como el principio de derecho específico para la materia de protección de datos personales, llamado a actuar de garante del respeto del resto de principios relativos al tratamiento, del RGPD, de la LOPDGDD y de la normativa sectorial en la materia, que obliga tanto al cumplimiento de la norma como a recoger las evidencias que permitan demostrarlo y que se concreta en la implementación de medidas adecuadas y eficaces.

Referencias bibliográficas

Bibliografía básica

Libros

DAVARA RODRÍGUEZ. M.A., DAVARA FERÁNDEZ DE MARCOS, E. y DAVARA FERNÁNDEZ DE MARCOS. L. *Manual de Derecho Informático*. 12ª ed. Navarra: Aranzadi, 2020.

MURGA FERNÁNDEZ, J.P. *et al*. *Protección de Datos, Responsabilidad Activa y Técnicas de Garantía*. 1ª ed. Madrid: Reus, 2018.

PIÑAR MAÑAS, J. *et al. Reglamento general de protección de datos*. 1ª ed. Madrid: Reus, 2016.

TRONCOSO REIGADA, A. *et al. Comentarios al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales*. 1ª ed. Navarra: Aranzadi, 2021.

Revistas

ALAMILLO DOMINGO, I. «El Esquema Nacional de Seguridad y el cumplimiento del artículo 32 del RGPD en el ámbito local». *La ley digital*. 2019, núm. 8799.

BAJO ALBARRACÍN, J.C. «Consideraciones sobre el principio de responsabilidad proactiva y diligencia (*accountability*). Experiencias desde el Compliance». *La ley digital*, núm. 123.

CUMBRERAS AMARO, M. «La seguridad de los datos personales y la obligación de notificar las brechas de seguridad». *Revista de Derecho, Empresa y Sociedad (REDS)*. 2020, núm. 16, pp. 151–162. ISSN 2340–4647.

DAVARA FERNÁNDEZ DE MARCOS, E. «La evaluación de impacto en protección de datos: aspectos de interés». *Actualidad Administrativa*, marzo 2018, núm.4. ISSN 1130-9946.

GAMERO CASADO, E. «El Delegado de Protección de Datos en las Administraciones públicas: Ombudsman de los datos personales». *La Administración al día*, 31 enero 2019, [consulta: 16 de marzo 2021]. Disponible en: http://laadministracionaldia.inap.es/noticia.asp?id=1509261

GONZÁLEZ, P.A. «Responsabilidad proactiva en los tratamientos masivos de datos». *Dilemata*. 2017, núm. 24, pp. 115–129. ISSN 1989–7022.

MIGUEL PÉREZ, J.C.« Alcance, profundidad y metodología del análisis de riesgos en el Reglamento General de Protección de Datos». *LA LEY privacidad*. 2020, núm.4, sección Ciberseguridad. ISSN-e 2659-8698.

RALLO LOMBARTE, A. «HACIA UN NUEVO SISTEMA EUROPEO DE PROTECCIÓN DE DATOS| LAS CLAVES DE LA REFORMA». *Revista de Derecho Político (UNED)*. 2012, núm. 85, pp. 14–56. ISSN 02119779X.

ROMERO RUIZ, A. «LA RESPONSABILIDAD PROACTIVA DE LAS ADMINISTRACIONES PÚBLICAS EN LA PROTECCIÓN DE DATOS PERSONALES». *Revista Vasca de Gestión de Personas y Organizaciones Públicas*. 2020, núm. 18, pp. 138–153. ISSN 2173–6405.

TRONCOSO REIGADA, A. «HACIA UN NUEVO MARCO JURÍDICO EUROPEO DE LA PROTECCIÓN DE DATOS PERSONALES». *Revista española de derecho europeo*. 2012, núm.43, pp. 25–184. ISSN 1579–6302.

Bibliografía complementaria

Libros

DE CASTRO CID, B., *Nuevas lecciones de Teoría del Derecho*. Madrid: Editorial Universitas, 2002.

Revistas

COMANDUCCI, P.«PRINCIPIOS JURÍDICOS E INDETERMINACIÓN DEL DERECHO». Doxa. 1998, núm. 21, vol. 2 (1998), pp. 89–104. ISSN 0214–8876.

MARTÍNEZ ESTAY. J.I. «LOS CONCEPTOS JURÍDICOS INDETERMINADOS EN EL LENGUAJE CONSTITUCIONAL». *Revista de derecho político (UNED)*. 2019, núm. 105, pp. 161–196. ISSN 0211–979X.

REBOLLO PUIG, M. «Los principios generales del derecho (atrevimiento atribulado sobre su concepto, funciones e inducción)». *La ley digital*, núm. 1122.

Otros documentos

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *CÓDIGO DE BUENAS PRÁCTICAS EN PROTECCIÓN DE DATOS PARA PROYECTOS BIG DATA* [en línea]. AEPD, 2019, [consulta: junio 2021]. Disponible en: https://www.aepd.es/sites/default/files/2019-09/guia-codigo-de-buenas-practicas-proyectos-de-big-data.pdf

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Gestión del riesgo y evaluación de impacto en tratamientos de datos personales* [en línea]. AEPD, 2021, [consulta: julio 2021]. Disponible en:

https://www.aepd.es/es/documento/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Guía del Reglamento General de Protección de Datos para Responsables de Tratamiento* [en línea]. AEPD, 2018, [consulta: mayo 2021]. Disponible en:

https://www.aepd.es/es/documento/guia–rgpd–para–responsables–de–tratamiento.pdf–0

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Guía de Protección de Datos desde el Diseño* [en línea]. AEPD, 2019, [consulta: mayo 2021]. Disponible en:

https://www.aepd.es/sites/default/files/2019-11/guia-privacidad-desde-diseno.pdf

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Guía de Protección de Datos por Defecto* [en línea]. AEPD, 2020, [consulta: mayo 2021]. Disponible en:

https://www.aepd.es/sites/default/files/2020-10/guia-proteccion-datos-por-defecto.pdf

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Guía para la gestión y notificación de brechas de seguridad* [en línea]. AEPD, 2018, [consulta: mayo 2021]. Disponible en:

https://www.aepd.es/sites/default/files/2019-09/guia-brechas-seguridad.pdf

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Guía Práctica de Análisis de Riesgos en los Tratamientos de Datos Personales Sujetos al RGPD* [en línea]. AEPD, 2018, [consulta: mayo 2021]. Disponible en:

https://www.aepd.es/es/documento/guia–analisis–de–riesgos–rgpd.pdf

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Guía Práctica para las Evaluaciones de Impacto en la Protección de los Datos Sujetos al RGPD* [en línea]. AEPD, 2018, [consulta: mayo 2021]. Disponible en:

https://www.aepd.es/es/documento/guia–evaluaciones–de–impacto–rgpd.pdf

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Listado de Cumplimiento Normativo* [en línea]. AEPD, 2018, [consulta: mayo 2021]. Disponible en:

https://www.aepd.es/es/documento/guia–listado–de–cumplimiento–del–rgpd.pdf

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Tecnologías y Protección de Datos en las AA.PP.* [en línea]. AEPD, 2020, [consulta: mayo 2021]. Disponible en:

https://www.aepd.es/sites/default/files/2020-11/guia-tecnologias-admin-digital.pdf

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Requisitos para Auditorías de Tratamientos que incluyan IA* [en línea]. AEPD, 2021, [consulta: mayo 2021]. Disponible en: https://www.aepd.es/sites/default/files/2021-01/requisitos-auditorias-tratamientos-incluyan-ia.pdf

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *El Delegado de Protección de Datos en las Administraciones Públicas* [en línea]. AEPD, 2019, [consulta: mayo 2021]. Disponible en: https://www.aepd.es/sites/default/files/2019-09/funciones-dpd-en-aapp.pdf

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *El enfoque de riesgos en el Reglamento* [en línea]. Blog AEPD, 15 de diciembre de 2018, [consulta: mayo 2021]. Disponible en: https://www.aepd.es/es/prensa-y-comunicacion/blog/el-enfoque-de-riesgos-en-el-reglamento

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *El Manual del DPD* [en línea]. AEPD, 2019, [consulta: abril 2021]. Disponible en: https://www.aepd.es/sites/default/files/2019–12/El%20Manual%20del%20DPD%20–%20KORFFGEORGES%20–%20ESP.pdf

AGENCIA ITALIANA DE PROTECCIÓN DE DATOS. *El Manual del DPD* [en línea]. T4DATA, 2019, [consulta: mayo 2021]. Disponible en: https://www.aepd.es/sites/default/files/2019-12/El%20Manual%20del%20DPD%20-%20KORFFGEORGES%20-%20ESP.pdf

COMITÉ EUROPEO DE PROTECCIÓN DE DATOS. *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default* [en línea]. EDPB, 2020, [consulta: mayo 2021]. Disponible en: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS- CENIL-. Les outils de la conformité [en línea]. CENIL, 2021, [consulta: mayo 2021]. Disponible en: https://www.cnil.fr/fr/les-outils-de-la-conformite

CONFERENCIA INTERNACIONAL DE AUTORIDADES DE PROTECCIÓN DE DATOS Y PRIVACIDAD. Estándares Internacionales sobre Protección de Datos Personales y Privacidad (Resolución de Madrid). [en línea]. UE, 2009, [consulta: mayo 2021]. Disponible en: https://edps.europa.eu/sites/edp/files/publication/09–11–05_madrid_int_standards_es.pdf

GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29. *Dictamen 01/2012 sobre las propuestas de reforma de la protección de datos* [en línea]. GT29, 2012, WP 191, [consulta: abril 2021]. Disponible en: https://ec.europa.eu/justice/article–29/documentation/opinion–recommendation/files/2012/wp191_es.pdf

GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29. *Dictamen 3/2010 sobre el principio de responsabilidad* [en línea]. GT29, 2010, WP 173, [consulta: abril 2021]. Disponible en: https://ec.europa.eu/justice/article–29/documentation/opinion–recommendation/files/2010/wp173_es.pdf

GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29. *Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679* [en línea]. GT29, 2017, WP 248, [consulta: mayo 2021]. Disponible en:

https://www.aepd.es/sites/default/files/2019-09/wp248rev01-es.pdf

GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29. *Directrices sobre los delegados de protección de datos (DPD)* [en línea]. GT29, 2016, WP 243, [consulta: mayo 2021]. Disponible en: https://www.aepd.es/sites/default/files/2019-09/wp243rev01-es.pdf

GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29. *The Future of Privacy* [en línea]. GT29, 2009, WP 168, [consulta: mayo 2021]. Disponible en:

https://ec.europa.eu/justice/article–29/documentation/opinion–recommendation/files/2009/wp168_en.pdf

SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS. *Accountability on the ground: Guidance on documenting processing operations for EU institutions, bodies and agencies* [en línea]. EDPB, 2019, [consulta: mayo 2021]. Disponible en: https://edps.europa.eu/data-protection/our-work/publications/guidelines/*accountability*-ground-provisional-guidance_en

THE UK'S INDEPENDENT AUTHORITY -ICO-. *Guide to the general date protection regulation* [en línea]. ICO, [consulta: mayo 2021]. Disponible en: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/*accountability*-and-governance/

Normativa citada

Nacional

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. *Boletín Oficial de Estado*, de 6 de diciembre de 2018, núm. 294, pp. 119788–119857.

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. *Boletín Oficial del Estado*, de 14 de diciembre de 1999, núm. 298, pp. 43088–43099. (Derogada).

Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal. *Boletín Oficial del Estado*, de 31 de octubre de 1992, núm. 262, pp. 3703–37045. (Derogada).

Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. *Boletín Oficial del Estado*, de 19 de enero de 2008, núm. 17.

Internacional de la UE

Reglamento (CE) n.º 45/2001 del Parlamento Europeo y de Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos, de 12 de enero de 2001, serie L, núm. 8 ,pp. 1-22 (Derogado).

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), de 4 de mayo de 2016, serie L, núm. 119, p. 1.

Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE, de 21 de noviembre de 2018, serie L, núm. 295, pp. 39-98.

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. *Diario Oficial de las Comunidades Europeas*, 23 de noviembre de 1995, serie L, núm. 281, p.31. (Derogada).

Jurisprudencia referenciada

Sentencia de la Audiencia Provincial de Zaragoza, de 11 de diciembre de 2018 (Roj: SAP Z 2551/2018 - ECLI: ES:APZ:2018:2551).

Sentencia de la Audiencia Nacional, de 15 de febrero de 2019 (Roj: SAN 387/2019 - ECLI:ES:AN:2019:387).

Listado de abreviaturas

AEPD: Agencia Española de Protección de Datos.

Art.: Artículo.

Arts.: Artículos.

CEPD: Comité Europeo de Protección de Datos.

DPD: Delegado de Protección de Datos.

DPO: *Data Protection Officer.*

EDPB: European Data Protection Board

EIPD: Evaluación de Impacto de Protección de Datos.

EM: Estados Miembros.

GT29: Grupo de Trabajo del artículo 29.

LOPD: Ley Orgánica 15/1999,de 13 de diciembre, de Protección de Datos de Carácter Personal.

LOPDGDD: Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

OCDE: Organización de Cooperación y Desarrollo Económicos.

PbD: *Privacy by Design*.

PDpD: Protección de datos por defecto.

PIA: *Privacy Impact Assessment*

RAT: Registro de actividades de tratamiento.

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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), en vigor desde el 25 de mayo y de obligado cumplimiento desde el 25 de mayo de 2018.

RLOPD: Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

TFM: Trabajo Fin de Máster.

UE: Unión Europea.