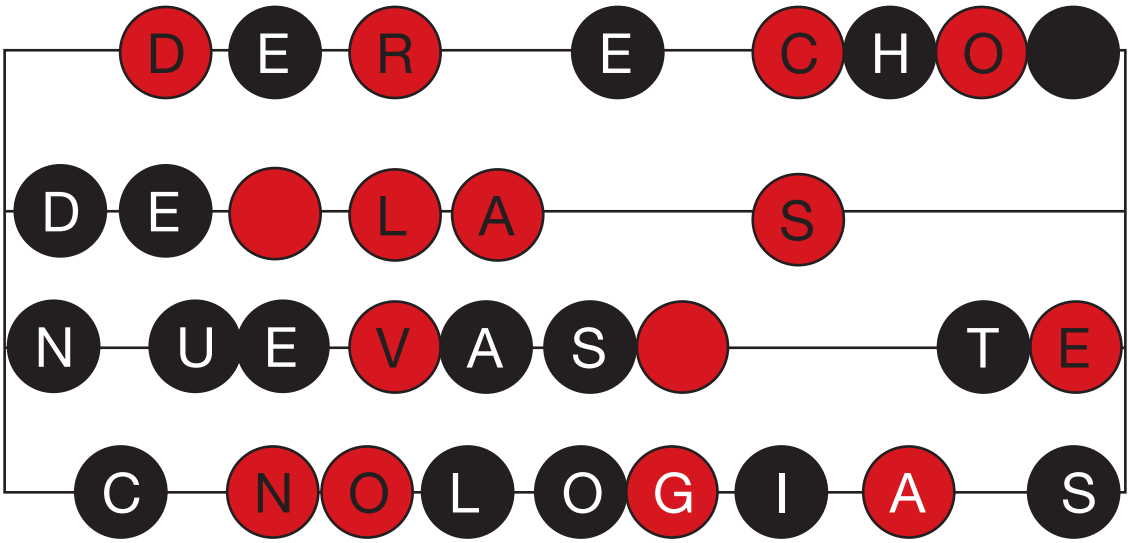

PROTECCIÓN DE DATOS, RESPONSABILIDAD ACTIVA Y TÉCNICAS DE GARANTÍA

CURSO DE «DELEGADO DE PROTECCIÓN DE DATOS»

Adaptado a la nueva Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

Directores:

Juan Pablo Murga Fernández

Profesor Ayudante Doctor de Derecho Civil (Contratado Doctor acr.), Universidad de Sevilla

María de los Ángeles Fernández Scagliusi

Profesora Ayudante Doctora de Derecho Administrativo (Contratada Doctora acr.), Universidad de Sevilla

Manuel Espejo Lerdo de Tejada

Catedrático de Derecho Civil, Universidad de Sevilla

Coordinadores:

Sara Lorenzo Cabrera

Personal Docente Investigador de la Universidad de Sevilla

Adrián Palma Ortigosa

Contratado Pre Doctoral de la Generalitat Valenciana, Universidad de Valencia

REUS
EDITORIAL

COLECCIÓN DE DERECHO DE LAS NUEVAS TECNOLOGÍAS

Directores:

Juan Pablo Murga Fernández
Profesor Ayudante Doctor de Derecho Civil, Universidad de Sevilla

María de los Ángeles Fernández Scagliusi
Profesora Ayudante Doctora de Derecho Administrativo, Universidad de Sevilla

Manuel Espejo Lerdo de Tejada
Catedrático de Derecho Civil, Universidad de Sevilla

Coordinadores:

Sara Lorenzo Cabrera
Personal Docente Investigador de la Universidad de Sevilla

Adrián Palma Ortigosa
Contratado Pre Doctoral de la Generalitat Valenciana, Universidad de Valencia

CURSO DE «DELEGADO DE PROTECCIÓN DE DATOS»

Adaptado al Proyecto de Ley Orgánica de Protección de Datos de 10 de noviembre de 2017

Dominio I
Fernández Scagliusi, María de los Ángeles
Lorenzo Cabrera, Sara
Murga Fernández, Juan Pablo
Palma Ortigosa, Adrián
Tomás Tomas, Salvador
Trujillo Cabrera, Carlos

Dominio II
De la Prada Espina, Diego
Romero Ternero, Mª Carmen

Dominio III
De la Prada Espina, Diego
Romero Ternero, Mª Carmen

REUS
EDITORIAL

Madrid, 2018

CAPÍTULO 7
RESPONSABILIDAD PROACTIVA

Sara Lorenzo Cabrera
Personal Docente Investigador de la Universidad de Sevilla
Adrián Palma Ortigosa
Contratado Pre Doctoral. Generalitat Valenciana. Universidad de Valencia
Carlos Trujillo Cabrera
Profesor Ayudante Doctor (acreditado Contratado Doctor). Universidad de La Laguna

1. PRIVACIDAD DESDE EL DISEÑO Y POR DEFECTO. PRINCIPIOS FUNDAMENTALES

1.1. Introducción

Las nociones sobre privacidad desde el diseño y por defecto (en sus siglas en inglés «*privacy by design*» y «*privacy by default*», respectivamente) fueron ideadas como tal por Ann Cavoukian en la década de los 90 quien, como directora de información y privacidad de Ontario (Canadá), quiso dar una respuesta metodológica que contrarrestara el factor de riesgo que suponía la tecnología de la información en la privacidad de los ciudadanos.

De acuerdo con su teoría, y muy brevemente, la noción de privacidad desde el diseño nos advierte de que el cumplimiento de la normativa de protección de datos es insuficiente para preservar la privacidad de los ciudadanos. Aunque existan normas sobre protección de datos y estas se cumplan no se conseguirá una protección real y plena de los datos personales. Para que ello suceda, defiende Ann Cavoukian, la garantía de privacidad debe convertirse en el modo de funcionamiento de la organización, es decir, debe quedar literalmente incrustada en el diseño de todo sistema o tecnología de la información, en las prácticas empresariales y en el diseño físico e infraestructura en red que en su caso se desarrollen.

De esta manera, esta nueva metodología requiere, como punto de partida, que las compañías u organizaciones (públicas y privadas) integren la privacidad desde el inicio, desde la fase preliminar del diseño de aquellos procesos o sistemas tecnológicos que conllevan un tratamiento de datos. Una vez la garantía de privacidad se convierte en la pieza clave de la arquitectura del proceso o sistema de tratamiento de datos, actuará durante todo el ciclo de vida de la información. Su implementación, por tanto, no sólo asegura que los ciudadanos tomen el control de su propia información personal, gracias a las exigencias de transparencia y trazabilidad del sistema, sino que se convierte en un valor predeterminado de la compañía por la que obtiene una ventaja competitiva y sostenible en el mercado.

Hay que destacar también que estos conceptos de privacidad desde el diseño y por defecto dan un giro de tuerca a las tecnologías de protección de la intimidad (conocidas como las PETs) que, según Ann Cavoukian, han quedado superadas por el imparable despliegue de las nuevas tecnologías. Las PETs fueron promovidas en 2007 por la Comisión Europea como sistema coherente de medidas TIC que protege el derecho a la intimidad, suprimiendo o reduciendo al mínimo la recogida de los datos personales o evitando el tratamiento innecesario o indeseado de tales datos, sin menoscabo de la funcionalidad del sistema de información. Como vemos, su definición va muy en la línea de lo que se concibe actualmente como «*privacy by default*», que es una noción consustancial a la propia idea de incorporar la privacidad desde el diseño.

Aunque la noción de privacidad desde el diseño surge en Canadá, la Directiva 95/46/CE, actualmente derogada, ya incorporaba tímidamente algunas previsiones en tal sentido. Valga como muestra su artículo 17 que obligaba a los responsables del tratamiento a que aplicaran salvaguardas tecnológicas en el diseño y funcionamiento de las TIC. Más explícito fue su considerando 46 que exigía la adopción de medidas técnicas y de organización apropiadas «tanto en el momento de la concepción del sistema de tratamiento como en la aplicación de los tratamientos, sobre todo con objeto de garantizar un nivel de seguridad adecuado (…)».

No obstante, pese a las anteriores referencias, no se hace una apuesta segura por la incorporación de la protección de datos desde el diseño y por defecto en el espacio europeo hasta el documento del GT29 de 1 de diciembre de 2009 (WP 28 02356/09/EN). En él se puso de manifiesto a la Comisión que, si bien las disposiciones y principios de la Directiva eran útiles y pertinentes (como, por ejemplo, los principios del art. 6: licitud y equidad, limitación de la finalidad, pertinencia, exactitud, plazo de conservación, responsabilidad) para la promoción de la privacidad desde el diseño, en la práctica, con el avance imparable de las nuevas tecnologías, no eran suficientes para garantizarla. A raíz de esta constatación, el GT29 defendió con firmeza que la protección de los datos debía implantarse desde la etapa de creación de los procedimientos y sistemas informáticos (privacidad desde el diseño). Y además añadía que este principio debía ser un compromiso compartido entre los diseñadores y productores de tecnología, así como de los responsables del tratamiento, que deben decidir sobre la adquisición y el uso de las TIC.

Como veremos más adelante el RGPD (art. 25) configura la privacidad desde el diseño y por defecto como una obligación exclusivamente del responsable que va a tratar datos personales, sin hacer mención a la posible corresponsabilidad de los diseñadores y productores de tecnología que el GT29 recomendó en su informe.

En la Conferencia anual sobre protección de datos y autoridades de control, celebrada en Israel en el año 2010, se consagra a escala internacional el principio de privacidad desde el diseño como el «componente esencial de la protección fundamental de la privacidad». Partiendo de esta premisa, se invita a todas las autoridades de control en materia de protección de datos a promover y fomentar la implantación de este nuevo paradigma en la política y la legislación de sus respectivas jurisdicciones.

Hemos señalado los hitos más importantes sobre la institución que nos proponemos analizar, con la finalidad de subrayar que el protagonismo que adquiere el principio de privacidad desde diseño en el nuevo RGPD no trae causa de la generación espontánea; muy al contrario, responde a una intensa y comprometida labor de difusión y asesoramiento de las instituciones internacionales y europeas (como el GT29), así como de las autoridades de control de los Estados, encaminada al mejoramiento de las TIC y de las prácticas empresariales respecto a la protección de los datos personales de los ciudadanos.

1.2. Principios fundamentales

El modelo de privacidad desde el diseño —PbD—, tal y como fue diseñado por Ann Cavoukian, se rige por siete principios fundacionales:

1. Proactivo y preventivo

Se trata de un sistema basado en prevenir los riesgos, no espera a que estos se materialicen, ni ofrece remedios para resolver las vulneraciones que se produzcan en materia de protección de datos. En resumen, la PbD actúa antes del suceso, no después. De esta manera, pasamos de un modelo reactivo, especialmente pensado para actuar en casos de incumplimiento normativo, a un modelo preventivo, regido por el conocido principio de precaución, que como recuerda Duaso Calés es propio del derecho medioambiental, que traslada sus esfuerzos al análisis anticipatorio de los riesgos y a una reflexión ética sobre las consecuencias que pudiera provocar en la privacidad de los afectados la adopción de una u otra medida técnica y organizativa.

El modelo de PbD no tendría carácter preventivo si no se supeditara a la metodología basada en el análisis de riesgos. Para prevenir los riesgos hay que saber cuáles son, es decir, identificarlos y actuar de acuerdo con la extensión y el alcance que estos determinen. En otras palabras, Volpato explica que es necesario evaluar todos los procesos y flujos de información previstos en el sistema y analizar sus implicaciones en privacidad desde un punto de vista holístico, preventivo y con un foco más allá del marco jurídico vigente.

Al mismo tiempo, este principio rector de precaución o prevención solo se podrá llevar a cabo correctamente si los creadores de un sistema de información y comunicación o de una operación de tratamiento mantienen una gobernanza proactiva, en la que no basta con cumplir la normativa en materia de protección de datos, sino que además deben demostrar que efectivamente lo hacen. Este nuevo paradigma sobre la responsabilidad (*accountability*) de los tratadores de datos personales se incorpora en el artículo 5.2 del RGPD como el principio de responsabilidad activa, que luego tendremos ocasión de retomar.

En definitiva, destaca la relación de interdependencia que existe entre el principio de prevención y de proactividad, ambos se retroalimentan entre sí, concibiéndose imprescindibles el uno para el otro.

2. Privacidad como configuración predeterminada

La protección de los datos personales se preservará de forma automática, sin necesidad de que el afectado por dicho tratamiento u operación tenga que realizar una determinada acción para que se garantice su privacidad. La privacidad forma parte del sistema, por lo que es el propio sistema el que está programado de forma predeterminada y automática, con base en el principio de prevención, para actuar ante cualquier riesgo que pueda afectar a los datos personales de los afectados. Estos últimos simplemente confían en el correcto funcionamiento del sistema de PbD, sin exigirles ninguna actuación para proteger sus datos.

3. Privacidad integrada en el diseño

Idea central del modelo de PbD, la privacidad no es un elemento complementario del proceso de diseño y construcción de los sistemas informáticos, de las infraestructuras en red y de las prácticas empresariales, sino la raíz y esencia de los mismos, constituyendo su parte integral sin reducir la funcionalidad del sistema.

4. Plena funcionalidad

Tradicionalmente, se ha considerado que la incorporación al sistema de medidas de seguridad y de protección de los datos personales va en detrimento del control y la funcionalidad de los sistemas tecnológicos. Desde este enfoque, ambos valores e intereses legítimos se excluyen mutuamente, dando lugar a un modelo basado en la paralizante dicotomía «seguridad-intimidad». Si se apuesta por la protección de la privacidad, se sacrifica el avance tecnológico y viceversa.

Con el surgimiento de las Tecnologías de protección del derecho a la intimidad (PETs) o técnicas garantes esta dicotomía comienza a desestabilizarse. Pero no lo hace del todo hasta la aparición del sistema de PbD, por el que todos los intervinientes salen beneficiados; literalmente «todos ganan». En este escenario se promueve el diálogo entre diseñadores de tecnología, empresarios y ciudadanos, tal y como apunta Duaso Calés, ya que es el único camino para proteger de forma efectiva los derechos fundamentales que pueden verse afectados por la tecnología y para que en ningún caso se vea frenado su desarrollo. Todos los acto-

res intervinientes están implicados en la búsqueda del equilibrio entre privacidad y seguridad.

5. Seguridad de extremo a extremo y protección durante todo el ciclo de vida

1. La privacidad por diseño garantiza la gestión de la seguridad y de la protección de la información personal de principio a fin del tratamiento. De esta manera, todos los actos de tratamiento (desde la recogida hasta la destrucción) de datos personales mantendrán un nivel oportuno de seguridad que permanecerá inalterado durante todo el ciclo de vida de la información, de un extremo a otro de su existencia.

6. Visibilidad y transparencia

La metodología de PbD implica además que cuando se vaya a realizar un tratamiento de datos personales, todas las operaciones programadas deben ser visibles y puestas en conocimiento de los usuarios. Esta idea conforma el derecho de información (arts. 13 y 14 del RGPD) y presupone que los datos personales tienen que ser tratados de manera lícita, por supuesto, pero además transparente, de modo que el interesado sea conocedor en todo momento de la finalidad del tratamiento y las distintas operaciones que se llevan a cabo sobre su información personal. El principio de transparencia se introduce por primera vez en el artículo 5.1.a) del RGPD, ya que no constaba expresamente en la Directiva 95/46/CE.

7. Respeto por la privacidad del usuario

En relación con el principio anterior, el usuario cuyos datos son objeto de tratamiento es la pieza central del sistema basado en la PdD. Todo queda configurado conforme al interés superior de aquel, por lo que se le concede un haz de facultades y derechos, así como oportunos remedios ante el incumplimiento.

1.3. Implementación en el artículo 25 del Reglamento General de Protección de Datos

Resulta interesante analizar cómo ha quedado configurada la privacidad desde el diseño y por defecto en el RGPD. Su implementación respeta los principios fundamentales que previamente hemos expuesto, pero también presenta algunas particularidades que debemos conocer.

1.3.1. Privacidad desde el diseño

En relación con la privacidad desde el diseño, el artículo 25.1 del RGPD establece que «teniendo en cuenta el estado de la técnica, el coste de aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto

en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados».

Atendiendo a su tenor literal, merece la pena exponer las siguientes consideraciones:

a) En primer lugar, la obligación de aplicar medidas técnicas y organizativas apropiadas que cumplan con la privacidad desde el diseño recae exclusivamente sobre el responsable del tratamiento, debido a que es dicho sujeto, conforme a la definición del artículo 4.7) del RGPD, el único que ostenta el monopolio y la capacidad de decisión sobre los «medios» que se ponen al servicio del tratamiento de datos personales. Por su parte, el encargado del tratamiento, si lo hubiera, simplemente tendrá la obligación de asistirle y cooperar con él en caso de que fuera necesario.
b) En segundo lugar, con carácter previo a la adopción de medidas de carácter técnico y organizativo que cumplan con la protección de datos desde el diseño y por defecto, el responsable deberá realizar una evaluación teniendo en cuenta los siguientes factores:
   El estado de la técnica.
   - El coste de la aplicación.
   - La naturaleza, ámbito, contexto y fines del tratamiento.
   - Los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de personas físicas.

Se aprecia de forma positiva que al responsable del tratamiento se le conceda en esta materia un amplio margen de decisión, puesto que además de atender a los aspectos puramente tecnológicos de la medida (estado de la técnica), también debe sopesar el coste económico de llevarla a cabo (coste de la aplicación). Ahora bien, tanto el factor tecnológico como el económico quedarán fuertemente condicionados por las conclusiones que se extraigan del previo análisis de los riesgos que las operaciones de tratamiento, en términos de probabilidad y gravedad, suponen para los derechos y libertades de las personas. El análisis de los riesgos (*risk-based approach* en su terminología inglesa) es el motor del RGPD, puesto que subyace no solo en la aplicación de los principios de protección desde el diseño y por defecto, sino también en el principio de responsabilidad activa (art. 5.2), en la elaboración del registro de actividades (art. 30), así como en la evaluación de impacto (art. 35).

En definitiva, el análisis de los riesgos va a predeterminar la línea de actuación que debe seguir el responsable del tratamiento. Desde esta perspectiva, si los riesgos para los derechos y libertades de las personas son altos, el responsable

tendrá que adoptar medidas probablemente más onerosas y tecnológicamente más avanzadas para conseguir que desde el diseño del tratamiento los medios utilizados sean respetuosos con la normativa de protección de datos.

c) En tercer lugar, el responsable del tratamiento puede adoptar las medidas técnicas y organizativas para cumplir con el principio de protección de datos desde el diseño y por defecto (art. 25) en dos momentos diferentes:
   - «en el momento de determinar los medios del tratamiento» o
   - «en el momento del propio tratamiento».

En general, el modelo de PbD se configura desde la implantación de medidas técnicas y organizativas en la fase inicial de desarrollo de la aplicación o del sistema de tratamiento de datos. Sorprende, por tanto, que el artículo mencionado permita que estas medidas sean adoptadas «en el momento del propio tratamiento», pues este constituye un momento temporal posterior al del diseño, lo que subvertir los principios rectores del modelo de PbD antes analizados.

d) En último lugar, el responsable tiene plena libertad para elegir las medidas técnicas y organizativas de privacidad desde el diseño que considere oportunas. Si bien, el Reglamento menciona, a título de recomendación, la idoneidad de las técnicas de seudonimización y de minimización de datos, así como la transparencia respecto a las funciones y al tratamiento, la habilitación de mecanismos para que los interesados puedan supervisar el tratamiento, etc. (cdo. 78).

1.3.2. Privacidad por defecto

La obligación de privacidad por defecto se regula en el 2 apartado del artículo 25 del RGPD. La protección de datos por defecto obliga al responsable a aplicar medidas técnicas y organizativas para garantizar que, por defecto, solo sean objeto de tratamiento los datos personales necesarios para cada fin específico del tratamiento. Esta obligación se aplicará a la cantidad de datos recogidos, a la extensión de su tratamiento, a su plazo de conservación y su accesibilidad.

En concreto, respecto de la accesibilidad, lo que se persigue con el cumplimiento de esta obligación proactiva es que, por defecto, los datos personales no sean accesibles, de forma automática, a un número indeterminado de personas físicas.

Asimismo, la privacidad por defecto aplica esencialmente el principio de calidad o minimización de los datos previstos en el artículo 5.1.c) del RGPD. Ello hace constar, así como expresó el GT29, que tanto la obligación de privacidad desde el diseño como la privacidad por defecto son obligaciones que se añaden a los principios materiales propios de la protección de datos (art. 5.1 RGPD) y que

son una expresión más del principio de responsabilidad proactiva o *accountability* (5.2 RGPD).

Finalmente, queda destacar que el Reglamento permite a los responsables del tratamiento acudir a los mecanismos de certificación para demostrar el cumplimiento de las obligaciones de protección de datos desde el diseño y por defecto (art. 25. 3 RGPD), tal y como se estudia con mayor detalle en este mismo capítulo.

2. EVALUACIÓN DE IMPACTO DE PROTECCIÓN DE DATOS Y LOS TRATAMIENTOS DE ALTO RIESGO

2.1. Consideraciones generales

El RGPD no define formalmente el concepto de «evaluación de impacto de protección de datos -EIPD-», también conocida por siglas en inglés *PIA* «*Privacy Impact Analysis*», motivo por el que tenemos que acudir a las directrices adoptadas por el GT29 (WP 248 rev.01). Según tales directrices, la EIPD es un «proceso concebido para describir el tratamiento, evaluar su necesidad y proporcionalidad y ayudar a gestionar los riesgos para los derechos y libertades de las personas físicas derivados del tratamiento de datos personales evaluándolos y determinando las medidas para abordarlos». En resumen, tal y como destaca el GT29, se trata de un instrumento de enorme importancia para dar efectivo cumplimiento al deber de rendición de cuentas (art. 5.2. y 24 RGPD) que pesa, principalmente, sobre el responsable del tratamiento.

En muy parecidos términos se pronunció en 2012 la Comisión Europea [SEC (2012) 72 final], definiendo a la EIPD como «un proceso a través del cual se hace un esfuerzo consciente y sistemático para evaluar los riesgos para la privacidad de las personas en las obtención, uso y divulgación de sus datos personales. Una EIDP ayuda a identificar los riesgos para la privacidad, predecir problemas y plantear soluciones».

A la vista de estas definiciones, resulta evidente que la EIPD es una herramienta de análisis integral que pretende «cartografiar» los riesgos y las amenazas de determinadas operaciones de tratamientos de datos personales para los derechos y libertades de las personas, con la finalidad última de prevenirlos activamente.

2.2. Obligación de realizar una evaluación de impacto: ¿en qué supuestos?

Al hilo del enfoque basado en el riesgo introducido por el art. 24 del RGPD, no es preceptiva la realización de una EIPD en todas y cada una de las operaciones de tratamiento que el responsable pretenda acometer. Tanto es así que solo será exigible cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, «*entrañe un alto*

riesgo» para los derechos y libertades de las personas físicas (arts. 35 y 36, así como los cdos. 89 y 91 del RGPD).

En particular, establece el apartado 3 del citado artículo 35, que la EIPD se requerirá por entrañar un alto riesgo en caso de:

a) evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;
b) tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, o
c) observación sistemática a gran escala de una zona de acceso público.

Esta lista de supuestos en los que es obligatoria la EIPD no tiene la pretensión de ser exhaustiva (por tanto, *numerus apertus*); esto significa que pueden existir operaciones de tratamiento de datos que, aún sin encajar literalmente en la enumeración anterior, suponen unos riesgos similarmente elevados que deben ser examinados mediante la citada evaluación.

Atendiendo fundamentalmente a los supuestos contenidos en el art. 35.3 del RGPD y a los cdos. 71, 75 y 91 RGPD, el GT29 ha elaborado un repertorio más concreto de criterios que permitirá al responsable del tratamiento valorar cuándo sus operaciones de tratamiento requieren una EIPD. En general, el GT29 considera que cuantos más criterios cumpla el tratamiento, más probable será que represente un alto riesgo para los derechos y libertades de los interesados y, por tanto, demande una EIPD independientemente de las medidas que el responsable contemple adoptar. Los criterios son los siguientes:

1. Evaluación o puntuación, incluida la elaboración de perfiles y la predicción, especialmente de «aspectos relacionados con el rendimiento en el trabajo, la situación económica, la salud, las preferencias o intereses personales, la fiabilidad o el comportamiento, la situación o los movimientos del interesado» (cdos. 71 y 91).

   (*v. gr*., una institución financiera que investigue a sus clientes en una base de datos de referencia de crédito o en una base de datos contra el blanqueo de capitales y la financiación del terrorismo o sobre fraudes, o una empresa de biotecnología que ofrezca pruebas genéticas directamente a los consumidores para evaluar y predecir los riesgos de enfermedad/salud, o una empresa que elabore perfiles de comportamiento o de mercadotecnia basados en el uso o navegación en su sitio web).

2. Toma de decisiones automatizada con efecto jurídico significativo o similar: se corresponde con aquel tratamiento destinado a tomar decisiones sobre los

interesados que produce «efectos jurídicos para las personas físicas» o que les afectan «significativamente de modo similar» [(art. 35, apartado 3, letra a)]. En sentido inverso, se desprende que no quedarán subsumidos en este supuesto aquellos tratamientos de datos personales con escaso o ningún efecto jurídico o de cualquier otra naturaleza sobre las personas físicas.

3. Observación sistemática: es el tratamiento de datos usado para observar, supervisar y controlar a los interesados, incluidos los datos recogidos a través de redes u «observación sistemática [...] de una zona de acceso público» [artículo 35, apartado 3, letra c)]. Este tipo de observación representa un criterio independiente porque los datos personales pueden ser recogidos en circunstancias en las que los interesados desconozcan quién está recopilando sus datos y cómo y con qué finalidad serán usados. Además, asegura el GT29, que puede resultar imposible para las personales evitar ser objeto de este tipo de tratamiento en espacios públicos o de acceso público.

Asimismo, merece un breve apunte el calificativo utilizado: «sistemática», ya que ha sido interpretado por el GT29 (16/EN WP 243) en uno o más de los siguientes sentidos:

— que se produce de acuerdo con un sistema;
— preestablecido, organizado o metódico;
— que tiene lugar como parte de un plan general de recogida de datos;
— que se lleve a cabo como parte de una estrategia.

(v.gr., el uso de un sistema de cámaras para controlar el comportamiento al volante en las autovías o una empresa que observa sistemáticamente las actividades de sus empleados, etc.).

4. Datos sensibles o datos muy personales: hace referencia a las categorías especiales de datos personales (art. 9 RGPD), así como datos personales relativos a condenas e infracciones penales (art. 10 RGPD).

(v.gr., un hospital general que guarda historiales médicos de pacientes o un investigador privado que guarda datos de delincuentes)

Al mismo tiempo, apunta el GT29 que nos podemos encontrar con tratamientos de determinados conjuntos de datos personales, denominados «datos sensibles», que, sin pertenecer a ninguna de las dos categorías anteriores, entrañan un aumento del riesgo o amenazan la integridad de los derechos y libertades de las personas por estar precisamente vinculados a actividades privadas, al ejercicio de un derecho fundamental, o porque tienen graves repercusiones en la vida cotidiana del interesado.

(*v.gr.*, las comunicaciones electrónicas cuya confidencialidad debe ser protegida, los datos de localización cuya recogida compromete la libertad de circulación o los datos financieros que podrían usarse para cometer fraude en los pagos).

En este punto, puede ser relevante para la EIPD que los datos ya se hayan hecho públicos por el interesado o por terceras personas.

5. Tratamiento de datos a gran escala: el RGPD no define formalmente el «tratamiento a gran escala»; si bien, nos puede servir de guía el cdo. 91 RGPD que identifica a este tipo de tratamiento con aquellas operaciones que «persiguen tratar una cantidad considerable de datos personales a nivel regional, nacional o supranacional y que podrían afectar a un gran número de interesados y entrañar probablemente un alto riesgo […]».

En cualquier caso, el GT29 recomienda que, a la hora de determinar si el tratamiento de datos se realiza o no a gran escala, se tengan en cuenta los siguientes parámetros:

«a. el número de interesados afectados, bien como cifra concreta o como proporción de la población correspondiente;
b. el volumen de datos o la variedad de elementos de datos distintos que se procesan;
c. la duración, o permanencia, de la actividad de tratamiento de datos;
d. el alcance geográfico de la actividad de tratamiento».

De conformidad con los elementos de análisis anteriores, el cdo. 91 RGPD deja fuera de la categoría de «tratamiento a gran escala» a aquellas operaciones de tratamiento de datos personales de pacientes o clientes realizadas por un solo médico u otro profesional de la salud o abogado. En estos supuestos, por tanto, la EIPD no debe ser obligatoria.

6. Asociación o combinación de conjuntos de datos: se refiere el GT29, por ejemplo, a la asociación o combinación de datos procedentes de varias operaciones de tratamiento realizadas para distintos fines o por responsables del tratamiento diferentes de manera que exceda las expectativas razonables del interesado. Para alcanzar un mayor entendimiento de este criterio se aconseja consultar el Dictamen del GT29 sobre la limitación de la finalidad, 13/EN WP 203, p. 24.

7. Datos relativos a interesados vulnerables: se hace referencia a este criterio en el cdo. 75 del RGPD y con él se da cuenta de que en determinadas circunstancias las personas pueden ser incapaces de autorizar o denegar el tratamiento de sus datos o de ejercer sus derechos, debido a un aumento del desequilibrio de poder entre los interesados y el responsable del tratamiento. Entre los

interesados vulnerables, cita el GT29, puede incluirse a niños, empleados, segmentos más vulnerables de la población que necesitan una especial protección (personas con enfermedades mentales, solicitantes de asilo, personas mayores, pacientes, etc.) y cualquier caso en el que se pueda identificar un desequilibrio en la relación entre la posición del interesado y el responsable del tratamiento.

8. Uso innovador o aplicación de nuevas soluciones tecnológicas u organizativas: el uso de una nueva tecnología, definida «en función del nivel de conocimientos técnicos alcanzado» (cdo. 91 RGPD), puede exigir la realización de una EIPD (art. 35, apartado 1, y los cdos. 89 y 91). El uso de dicha tecnología, tal y como comenta el GT29, puede implicar nuevas formas de recogida y utilización de datos, posiblemente con un alto riesgo para los derechos y libertades de las personas. De hecho, las consecuencias personales y sociales del despliegue de una nueva tecnología pueden ser desconocidas. Una EIPD ayudará al responsable del tratamiento a entender y abordar tales riesgos.

   (*v.gr.*, algunas aplicaciones del «Internet de las cosas» podrían tener un impacto significativo sobre la vida diaria y la privacidad de las personas y, por tanto, requieren una EIPD, como combinar el uso de huella dactilar y reconocimiento facial para mejorar el control físico de acceso, etc.).

9. Cuando el propio tratamiento «impida a los interesados ejercer un derecho o utilizar un servicio o ejecutar un contrato» (art. 22 y cdo 91 del RGPD). En este último supuesto el GT29 incluye a todas aquellas operaciones de tratamiento de datos destinadas a permitir, modificar o denegar el acceso de los interesados a un servicio o a un contrato. En nuestra opinión, este criterio no es más que una mera ejemplificación del criterio «2. Toma de decisiones automatizada con efecto jurídico significativo o similar» que ya ha sido abordado.

   (*v.gr.*, un banco investiga a sus clientes en una base de datos de referencia de crédito con el fin de decidir si les ofrece un préstamo).

En relación con este elenco de supuestos en que deberá realizarse preceptivamente la EIPD, el Reglamento impone a las autoridades de control la obligación de elaborar y publicar listas adicionales de otros tipos de operaciones de tratamiento de datos que tengan la consideración de alto riesgo. Estas listas deberán ser comunicadas al Comité por la vía del artículo 68 del RGPD.

Igualmente, aunque ya no con carácter preceptivo, las autoridades de control podrán establecer y publicar la lista de los tipos de tratamiento que no requieren EIPD relativas a la protección de datos (aptos. 4 y 5 del art. 35 del RGPD).

Hay que señalar, por último, que, si esas listas incluyen actividades de tratamiento que guardan relación con la oferta de bienes o servicios a interesados o con la observación del comportamiento de estos en varios Estados miembros, o

actividades de tratamiento que puedan afectar sustancialmente a la libre circulación de datos personales en la UE, las autoridades de control deberán aplicar el mecanismo de coherencia contemplado en el artículo 63 del RGPD.

2.2. ¿Quién es el sujeto obligado a realizar la EIPD y cuándo debe hacerlo?

El sujeto obligado a realizar la EIPD es el responsable del tratamiento (art. 35.1. RGPD); aunque más que elaborarla por sí mismo, tiene la obligación de garantizar que alguien (cualquier persona de dentro o de fuera de la organización) la lleve a cabo debidamente, siendo el responsable del tratamiento el que responderá en última instancia por la incorrecta realización de la referida tarea. No cabe duda de que esta específica obligación debe encuadrarse dentro del deber general de gestionar adecuadamente los riesgos que presenta el tratamiento de datos personales (art. 24 del RGPD).

El GT29 precisa que cuando la EIPD implique a corresponsables, de conformidad con el art. 26 RGPD, estos deben definir de forma clara y precisa sus respectivas obligaciones, debiendo expresar y compartir la información que sea útil para tal fin sin poner en peligro los derechos y libertades de los interesados y los secretos comerciales o de otra índole de naturaleza confidencial (*v.gr.*, protección de secretos comerciales, propiedad intelectual, información comercial confidencial).

Asimismo, se ha de señalar que el responsable del tratamiento no podrá emprender la EIPD sin antes recabar el asesoramiento jurídico-técnico del delegado de protección de datos, si ha sido nombrado, y, cuando proceda, la opinión de los interesados o de sus representantes, sin perjuicio de la protección de intereses públicos o comerciales o de la seguridad de las operaciones de tratamiento (apdos. 2 y 9 del art. 35 del RGPD).

Con respecto al momento temporal, la EIPD deberá hacerse «antes» de la puesta en marcha de las operaciones de tratamiento (art. 35.1 y 10, y cdos. 90 y 93 del RGPD), salvo cuando es un tratamiento que ya existe y que ya ha sido comprobado por la autoridad de control, en cuyo caso la EIPD debe realizarse antes de que sufra cambios importantes.

Este requisito temporal, de naturaleza claramente preventiva y en la línea del principio de responsabilidad proactiva del artículo 5.2. del RGPD, está íntimamente relacionada con los principios de protección desde el diseño y por defecto, ya que constituyen un verdadero proceso de reflexión que tiene lugar antes del inicio de las operaciones de tratamiento. La EIPD debe percibirse como un instrumento de ayuda en la toma de decisiones relativas al tratamiento (GT29).

2.3. Ámbito y contenido mínimo de la EIPD

La EIPD puede abarcar tanto una única operación de tratamiento como múltiples operaciones que sean similares en términos de naturaleza, alcance, contexto,

fines y riesgos. En línea con esta afirmación, el cdo. 92 del RGPD añade que «hay circunstancias en las que puede ser razonable y económico que una evaluación de impacto relativa a la protección de datos abarque más de un único proyecto, por ejemplo, en el caso de que las autoridades u organismos públicos prevean crear una aplicación o plataforma común de tratamiento, o si varios responsables proyectan introducir una aplicación o un entorno de tratamiento común en un sector o segmento empresarial o para una actividad horizontal de uso generalizado».

Por lo que se refiere al contenido mínimo de la evaluación de impacto, el Reglamento contempla un contenido mínimo, que trata los siguientes puntos:

a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento;
b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;
c) una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1, y
d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el RGPD teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

Por el contrario, el Reglamento no contempla ninguna metodología específica para su realización, pero puede servir de ayuda a estos efectos la «Guía sobre Evaluaciones de Impacto» actualizada y publicada por la AEPD.

En último lugar, basta con indicar que el cumplimiento de los códigos de conducta aprobados de conformidad con el artículo 40 del RGPD por el responsable o encargados correspondientes se tendrá debidamente en cuenta al evaluar las repercusiones de las operaciones de tratamiento realizadas por dichos responsables o encargados, en particular a efectos de la EIPD.

2.3. Revisión de la evaluación de impacto

El GT29 subraya que la EIPD es un proceso continuo, y no una medida excepcional o puntual, especialmente cuando una operación de tratamiento es dinámica y está sujeta a cambios permanentes. De esta manera, resulta aconsejable que en las políticas de protección de datos se prevean mecanismos de revisión de tales evaluaciones.

En este sentido, el apartado 11 del artículo 35 del RGPD dispone que «en caso necesario, el responsable examinará si el tratamiento es conforme con la evaluación de impacto relativa a la protección de datos, al menos cuando exista un cambio del riesgo que representen las operaciones de tratamiento».

2.4. Consulta previa

2.4.1. Supuestos de consulta previa

Si una EIPD muestra que las operaciones de tratamiento entrañan un alto riesgo que el responsable no puede mitigar con medidas adecuadas en términos de tecnología disponible y costes de aplicación, el responsable del tratamiento deberá consultar a la autoridad de control competente (art. 36.1. y cdo. 84 del RGPD).

También deben llevarse a cabo consultas previas con la autoridad de control competente en el curso de la tramitación de una medida legislativa o reglamentaria que establezca el tratamiento de datos personales, a fin de garantizar la conformidad del tratamiento previsto en el RGPD y, en particular, de minimizar el riesgo que implique el tratamiento para el interesado (art. 36.4 y cdo. 96 del RGPD).

Además de los dos casos anteriores, el Derecho de los Estados miembros podrá prever otros supuestos diferentes en los que se regule la obligación de los responsables del tratamiento de consultar a la autoridad de control y recabar su autorización previa en relación con el tratamiento que se lleve a cabo en el ejercicio de una misión realizada en interés público. En concreto, apunta el Reglamento cuando el tratamiento esté relacionado con la protección social y la salud pública (art. 36.5 del RGPD).

2.4.2. Sujeto obligado y procedimiento de consulta

La consulta previa regulada en el artículo 36 del RGPD es una obligación exclusiva del responsable del tratamiento (arts. 4.7) y 24 del RPGD) y que, en el momento de realizarla, tendrá que ir acompañada de toda la documentación siguiente:

a) en su caso, las responsabilidades respectivas del responsable, los corresponsables y los encargados implicados en el tratamiento, en particular en caso de tratamiento dentro de un grupo empresarial;
b) los fines y medios del tratamiento previsto;
c) las medidas y garantías establecidas para proteger los derechos y libertades de los interesados de conformidad con el Reglamento;
d) en su caso, los datos de contacto del delegado de protección de datos;
e) la evaluación de impacto relativa a la protección de datos establecida en el artículo 35 del RGPD, y
f) cualquier otra información que solicite la autoridad de control.

Una vez realiza la consulta previa por parte del responsable, y cuando la autoridad de control considere que el tratamiento previsto en el artículo 36.1 podría infringir la normativa de protección de datos (lo que sucederá cuando el responsable no haya identificado o mitigado adecuadamente el riesgo), tendrá la obliga-

ción de asesorar por escrito al responsable y, en su caso, al encargado, en un plazo de ocho semanas desde la solicitud de la consulta.

En el ejercicio de su función de asesoramiento, la autoridad de control podrá utilizar cualquiera de sus poderes mencionados en el artículo 58 del RGPD, entre ellos el de prohibir la operación de tratamiento (art. 36.2 del RGPD).

3. SEGURIDAD DE LOS DATOS PERSONALES

3.1. Introducción

Como ya se analizó en páginas anteriores, la seguridad es reconocida en el Reglamento como un principio relativo al tratamiento de los datos personales Art 5.1 f). Este principio exige que los datos sean tratados de tal manera que se garantice una seguridad adecuada. Consagrado dicho principio, este es posteriormente materializado y desarrollado en el Art 32 y ss del Reglamento. De esta forma, dicho precepto obliga tanto al responsable como el encargado del tratamiento a establecer todo tipo de medidas técnicas y organizativas apropiadas que garanticen un nivel de seguridad adecuado al riesgo. A la hora de implantar unas u otras medidas, el responsable y el encargado del tratamiento deberán de tener en cuenta entre otros aspectos; el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas. Es turno ahora de analizar algunas de las medidas a las que hace referencia el Reglamento.

3.2. Medidas técnicas y organizativas relativas a la seguridad del tratamiento

Entre las medidas a las que el Reglamento alude destacan:

a) La seudonimización y el cifrado de los datos: Art.32.1.a)

El Reglamento apuesta por la seudonimización y el cifrado como medidas adecuadas que pueden favorecer a una mayor garantía de la seguridad en el tratamiento de los datos. (Cods.28 y 83 respectivamente). Concretamente, la implantación del cifrado de datos como medida de seguridad puede exonerar al responsable de la obligación de comunicar a los interesados la existencia de un incidente o violación de seguridad. Art 34.1 a).

b) La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanente de los sistemas y servicios de tratamiento. Art. 32.1. b)

Es decir, se exige que las medidas que se implanten en las organizaciones

aseguren un acceso a los datos exclusivamente por aquellas personas que estén autorizadas (confidencialidad) que la información no sea alterada (integridad), que dicha información esté disponible cuando se necesite (disponibilidad), y que se establezca un sistema que sea capaz de recuperarse ante ataques o perturbaciones. (Resiliencia). Para que se puedan llevar a cabo estas medidas no solo se requerirá de la implantación de sistemas técnicos adecuados, sino que a su vez se necesita del desarrollo de medidas organizativas que favorezcan un correcto entendimiento y cumplimiento interno por parte del personal que se encarga de tratar los datos personales, algunas de estas medidas organizativas podrían ser; la asignación de responsabilidades, la concienciación en seguridad, la elaboración y mantenimiento de planes de contingencia, etc.

c) *La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico.* Art.32.1.c)

Muy relacionado con la resiliencia, este tipo de medidas busca facilitar la accesibilidad de los datos personales tanto por parte del responsable como del encargado del tratamiento para aquellos casos en los que el sistema haya sufrido un incidente, a su vez, esta capacidad disponibilidad también favorecerá a que en su caso los interesados pueden ejercer efectivamente los derechos y facultades que le brinda el RGPD.

d) *La implantación de procesos de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.* Art 32.1.d)

El Reglamento también incluye como medidas apropiadas de seguridad la implantación de auditorías de seguridad. En este sentido, el propio texto europeo exige que dentro del contenido mínimo del contrato entre responsable y encargado del tratamiento se prevea la implantación de auditorías de seguridad. Art 28.3h). Además, en aquellos casos en los que la organización disponga de un delegado de protección de datos, este deberá de llevar a cabo auditorías. Art 39.1 b). Junto con las auditorías tanto internas como externas, y muy relacionado con el principio de *accountability* o rendición de cuentas, en este apartado también se incluirán todo tipo de actuaciones que permitan monitorizar de forma continua y proactiva la seguridad del tratamiento, logrando con ello disminuir las posibles sanciones derivadas del incumplimiento de este tipo de medidas. Art 83.2 d).

e) *Llevanza de un registro de las actividades del tratamiento.* Art 30.

Ya explicado en páginas anteriores, la obligación de mantener registros de las actividades de tratamiento en determinadas organizaciones implica desde el punto de vista de la seguridad de los datos una descripción general de las medidas técnicas y organizativas de seguridad implantadas por el responsable y el encargado del tratamiento. Art 30.1 g). Este registro, y por lo que respecta a la seguridad de los datos, supondrá en la práctica una asimilación al documento de seguridad (DS)

que la norma española viene exigiendo al responsable del tratamiento. Art 88. Reglamento de desarrollo de la LOPD. Real Decreto 1720/2007, de 21 de diciembre.

f) Evaluación de impacto relativa a la protección de datos. Art 35

En lo que atañe a la seguridad de los datos personales, en los supuestos que se requiera de una evaluación de impacto, esta última deberá de contener una evaluación de los riesgos que puede comportar un determinado tratamiento para los derechos y libertades de los interesados y que medidas tiene previstas el responsable para combatir tales riesgos, concretamente, que medidas de seguridad tiene previstas. Art 35.7 apartados b y c.

Se puede apreciar por tanto que el Reglamento, y a diferencia de nuestra antigua legislación española que preveía un conjunto de medidas de seguridad en función de la naturaleza de los datos (medidas de nivel básico, medio o alto), no impone tal concreción, sino que la implantación de las medidas variará en función de los factores señalados previamente en el Art 32.1 y, de los riesgos que pueda comportar un tratamiento de datos específico. En este sentido, la no imposición de unas medidas de seguridad predefinidas puede resultar beneficiosa para las organizaciones debido a que estas tendrán una mayor flexibilidad a la hora de implantar unas u otras medidas. Sin embargo, esa misma indefinición de las medidas de seguridad, se puede convertir en un hándicap de las organizaciones al generarse un alto grado de incertidumbre por no conocer a ciencia cierta si las medidas que deciden implantar cumplen o no con la normativa sobre protección de datos.

Habida cuenta de ello, y derivado de estas nuevas exigencias de seguridad, lo lógico será que las organizaciones se adhieran a códigos de conducta sectoriales aprobados en su caso por las autoridades de control o el Comité Europeo de Protección de Datos donde se prevean tales medidas de seguridad adecuadas. Todo ello sin perjuicio de la necesidad de adoptar medidas concretas de seguridad para cada tratamiento particular que afronte una determinada organización. Por lo que se refiere a las Administraciones Publicas, la implantación de las medidas de seguridad estará marcada por los criterios establecidos en el Esquema Nacional de Seguridad (ENS) conforme a la Disposición Adicional Primera del Proyecto de Ley de Protección de datos

En definitiva, la importancia de adoptar medidas apropiadas que garanticen la seguridad de los datos se muestra como esencial en la medida que, no solo se protegerá correctamente el derecho fundamental a la protección de datos, sino que en principio se evitaran o al menos se tenderá a aminorar las posibles sanciones y responsabilidades derivadas de fallos de seguridad a la hora de implantar tales medidas técnicas y organizativas. Art 83. Y es que, no podemos olvidar que en la mayoría de los casos, la no implantación de medidas de seguridad apropiadas se manifestará a través de una brecha o violación de seguridad en el sistema previamente establecido, lo que supondrá dejar al descubierto las debilidades de la organización en el cumplimiento de dichas exigencias de seguridad.

4. LAS VIOLACIONES DE SEGURIDAD. NOTIFICACIÓN Y COMUNICACIÓN DE LAS VIOLACIONES DE SEGURIDAD

A diferencia de la Directiva 95/46, el Reglamento prevé la obligación por parte de los responsables de comunicar los incidentes o violaciones de seguridad de los datos personales. De este modo, el Reglamento, en el Art 4.12 define este concepto 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*. Es decir, tal definición engloba todo tipo de situaciones que pueden ir desde un ataque cibernético masivo a nivel mundial a una organización, hasta el robo de un portátil o un error a la hora de enviar una determinada información a un correo electrónico equivocado.

Pues bien, una vez que conocemos la definición de violación de seguridad, es turno de analizar los dos mecanismos que ha previsto el Reglamento a la hora de notificar/comunicar dichas violaciones de seguridad. De esta manera, la normativa europea distingue dos mecanismos en función de quién sea el receptor que recibe dicha información sobre el incidente o brecha de seguridad, esto es, la autoridad de control o los interesados. Previéndose en cada mecanismo, cómo y cuándo, se ha de informar a dichos sujetos de tal incidente. En este sentido conviene señalar, que la obligación de notificar y comunicar a las autoridades de control e interesados en caso de brecha de seguridad no es novedosa en el panorama legal europeo, así, el Art 4 de la Directiva 2002/58 e-privacy tras la modificación sufrida por la Directiva 2009/136/EC ya prevé tal obligación.

4.1. Notificación de una violación de seguridad. Art 33. RGPD

4.1.1. Sujeto al que se ha de notificar y deber de notificación

El Art 33 impone al responsable el deber de notificar a la autoridad de control aquellas situaciones en las que la organización sufra una violación de seguridad de los datos personales. Como regla general, dicha notificación deberá de realizarse sin dilación indebida y, de ser posible, en un plazo no superior a 72 horas desde el momento que ha tenido constancia el responsable de dicha violación. Así, si la notificación excede de dicho plazo, el responsable habrá de indicar los motivos de tal dilación. Se excepciona el deber de notificación en aquellos casos en los que el responsable considera improbable que dicha violación de seguridad constituye un riesgo para los derechos y libertades de las personas físicas. Por otro lado, cuando el incidente lo sufra el encargado del tratamiento, este último habrá de notificar sin dilación indebida al responsable de tal violación. Con esta última previsión se logra involucrar al encargado en el proceso de comunicación de incidentes de seguridad.

4.1.2 Contenido mínimo de la notificación

La notificación deberá de contener necesariamente:

1. Una descripción de la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.
2. El nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.
3. Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.
4. Descripción de las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

Tras la notificación, la autoridad de control correspondiente verificará las medidas correctivas adoptadas por el responsable y en su caso, le indicará que comunique dicho incidente a los interesados. Esta información podrá proporcionarse de forma escalonada cuando no sea posible hacerlo en el mismo momento de la notificación.

4.1.3. Otras obligaciones

El Art 33.4 establece la obligación del responsable de llevar un registro documental de todo incidente de seguridad de los datos que haya podido sufrir la organización, independientemente de que se haya procedido o no a la notificación de dicha brecha. Dicho registro permitirá a la autoridad de control verificar el cumplimiento de las exigencias relativas a la notificación de las violaciones de seguridad.

4.2. Comunicación de una violación de seguridad. Art 34

4.2.1. Sujeto al que se ha de comunicar y deber de comunicación

El Art. 34 establece el deber del responsable de comunicar al interesado la existencia de un incidente o brecha de seguridad en aquellos casos en los que sea probable que la violación de seguridad de los datos personales entraña un alto riesgo para los intereses y libertades de las personas físicas. Dicha comunicación habrá de realizarse sin dilación indebida, esto es, tan pronto como sea posible, no obstante, en determinados casos podrá justificarse una comunicación más tardía por la necesidad de aplicar medidas adecuadas que impidan violaciones de seguri-

dad de los datos personales continuas o similares (cdo.86), o por ejemplo, puedan obstaculizar investigaciones policiales relativas a tales incidentes de seguridad. (Cdo. 88)

4.2.2. Contenido mínimo de la comunicación.

La comunicación del incidente de seguridad deberá de describirse en un lenguaje claro y sencillo, debiendo contener como mínimo la misma información y medidas que se exigían al responsable en las notificaciones de incidentes de seguridad cuando el receptor era la autoridad de control, a excepción únicamente de aquella información referida al número aproximado de interesados afectados, las categorías y el número aproximado de registros de datos personales afectados. Art 34.2 en relación con el Art 33.3.a).

Por último, no será necesaria tal comunicación cuando se de alguno de los siguientes condicionantes: Art 34.3.

- El responsable hubiera adoptado medidas técnicas u organizativas apropiadas y estas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular las medidas que hagan ininteligibles los datos para aquellos que no estén autorizados a acceder a ellos, como sería el cifrado.
- Cuando el responsable haya tomado con posterioridad a la quiebra medidas técnicas que garanticen que ya no hay posibilidad de que el alto riesgo se materialice.
- Cuando la notificación suponga un esfuerzo desproporcionado, debiendo en estos casos sustituirse por medidas alternativas como puede ser una comunicación pública.

4.2.3. Otras obligaciones

En aquellos casos en los que el responsable no haya comunicado a los interesados el incidente de seguridad y la autoridad de control considere la probabilidad de que dicha violación entraña un alto riesgo, esta última podrá exigir al responsable que; o bien, proceda a tal comunicación del incidente, o bien, adopte alguna de las condiciones a las que aludíamos anteriormente en relación al Art 34.3.

4.2.4. Justificación de las comunicaciones

El objetivo esencial de la comunicación de los incidentes de seguridad a los interesados es permitir que estos puedan tomar medidas para protegerse de las consecuencias negativas que les puede generar tal brecha de seguridad, consecuencias que pueden desembocar en la causación de un daño material, pero también en perjuicios de naturaleza inmaterial. Perjuicios que en muchas situaciones

y a priori no se conocerán a ciencia cierta, y que podrán o no llegar a vislumbrarse a largo plazo. A modo de ejemplo, ante un incidente de seguridad que sufre una organización que trata datos genéticos o de salud, el titular de tales datos, puede que nunca llegue a conocer que, debido a ese incidente de seguridad, una entidad dedicada a los seguros se niegue a concertar un determinado seguro porque conoce de su historial médico, fruto del incidente que años antes sufrió la organización mencionada arriba.

5. CÓDIGOS DE CONDUCTA Y CERTIFICACIONES

Las ventajas de los mecanismos extrajudiciales de solución de conflicto fueron puestas de manifiesto por la propia Comisión Europea desde comienzos de la década de los 90, a lo que siguió, especialmente en el campo digital, una profunda promoción de los mismos como es el caso, por ejemplo, del artículo 16 de la Directiva 200/31/CE, del Parlamento Europeo y del Consejo, de 8 de junio, relativa a determinados aspectos jurídicos del comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico). En esta misma línea, establece ahora el considerando 77 RGPD que *"se podrían proporcionar directrices (…) para demostrar el cumplimiento por parte del responsable o del encargado del tratamiento, especialmente con respecto (…) a la identificación de buenas prácticas para mitigar el riesgo, que revistan, en particular, la forma de códigos de conducta aprobados, certificaciones aprobadas, directrices dadas por el Comité o indicaciones proporcionadas por un delegado de protección de datos"*.

De esta manera, los códigos de conducta y las certificaciones aprobadas se posicionan en el RGPD como mecanismos de autorregulación dirigidos a potenciar las garantías de los titulares de datos y a aumentar su confianza en que el tratamiento que se haga de los mismos será (como mínimo) el legalmente exigible.

5.1. Códigos de conducta

Siguiendo a Díaz-Romeral Gómez, es posible definir los códigos de conducta como aquellos acuerdos de buenas prácticas que no están impuestos por el Derecho de la Unión o el de un Estado miembro, pero sí aprobados por la autoridad pública de control competente y, en su caso, por el Comité Europeo de Protección de Datos (CEPD) o por la Comisión; y en los que se definen el comportamiento y las buenas prácticas de aquellos responsables y encargados del tratamiento que, mediante su adhesión al código, se comprometen a cumplir sus disposiciones. Estas disposiciones, por su parte, deberán estar orientadas a la correcta aplicación del RGPD, bajo la supervisión de un organismo acreditado por la autoridad de control en cada caso competente.

La Directiva 95/46/CE establecía en su artículo. 27 -y ya antes que ella lo había hecho la Ley Orgánica 5/1992, de 28 de octubre (LORTAD) en su artículo

31- que *"los Estados miembros y la Comisión alentarán la elaboración de códigos de conducta destinados a contribuir, en función de las particularidades de cada sector, a la correcta aplicación de las disposiciones nacionales adoptadas por los Estados miembros en aplicación de la presente Directiva"*. En un sentido similar se manifiesta hoy el considerando 98 RGPD cuando dispone que *"se debe incitar a las asociaciones u otros organismos que representen a categorías de responsables o encargados a que elaboren códigos de conducta, dentro de los límites fijados por el presente Reglamento, con el fin de facilitar su aplicación efectiva (…). Dichos códigos de conducta podrían en particular establecer las obligaciones de los responsables y encargados, teniendo en cuenta el riesgo probable para los derechos y libertades de las personas físicas que se derive del tratamiento"*.

Por ello, el artículo 40 RGPD principia afirmando que los Estados miembros, las autoridades de control, el CEPD y la Comisión promoverán la elaboración de códigos de conducta destinados a contribuir a la correcta aplicación del RGPD, teniendo en cuenta las características específicas de los distintos sectores de tratamiento y las necesidades específicas de las microempresas y las pequeñas y medianas empresas.

Tales códigos de conducta tienen por objeto facilitar la correcta aplicación del RGPD (*ex* considerando 98, transcrito más arriba) respecto de determinados extremos del mismo que se exponen de manera detallada en el apartado 2 del citado precepto, adaptando al concreto sector en que van a ser aplicadas las reglas genéricas contenida en el RGPD, y clarificando las obligaciones exigibles a responsables y encargados. E, indirectamente, demostrar que quienes los suscriben, al hacerlo voluntariamente, están cumpliendo efectivamente con las obligaciones que se derivan de dicho Reglamento (cdo. 81 RGPD). Así lo establece expresamente el artículo 24.3 RGPD cuando afirma que la adhesión a códigos de conducta aprobados servirá *"como elementos para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento"*, y en sentido similar, se manifiestan los artículos 28.5 RGPD (respecto del encargado), 32.3 RGPD (respecto de la seguridad), y 35.8 RGPD (respecto de la evaluación de las repercusiones de las operaciones de tratamiento realizadas por los responsables o encargados, en particular a efectos de la evaluación de impacto relativa a la protección de datos); lo que justifica que el artículo 83.2.j) RGPD tenga en cuenta estas adhesiones a la hora de decidir acerca de la imposición de una multa administrativa y su cuantía en cada caso individual, siempre, claro está, que no se trate de una mera adhesión formal, sino que efectivamente la conducta del responsable o encargado se haya ajustado a las recomendaciones contenidas en dicho código.

Una idea similar se puede encontrar en el artículo 32 LOPD, en el que reciben el nombre de *códigos tipo*, y establecen las condiciones de organización, régimen de funcionamiento, procedimientos aplicables, normas de seguridad del entorno, programas o equipos, obligaciones de los implicados en el tratamiento y uso de la información personal, así como las garantías, en su ámbito, para el ejercicio de los derechos de las personas con pleno respeto a los principios y dispo-

siciones normativa en materia de protección de datos. Y recuerda en su apartado tercero que *"los códigos tipo tendrán el carácter de códigos deontológicos o de buena práctica profesional"*.

Los códigos de conducta, por tanto, se constituyen como una suerte de buenas prácticas que buscan ofrecer mayor seguridad y confianza a las relaciones entre el responsable del tratamiento de los datos y el titular de los mismos.

El procedimiento para la creación y aprobación de un código de conducta parte de la presentación, por las asociaciones y demás organismos mencionados en artículo 40.2 RGPD, del proyecto de código o la modificación o ampliación pretendida a la autoridad de control que sea competente con arreglo al artículo 55 RGPD. En la tramitación de estos códigos, los promotores deberán consultar a todas las partes afectadas por los mismos, incluidos los interesados cuando sea posible, y tener en cuenta las consideraciones transmitidas y las opiniones manifestadas por todos los afectados en respuesta a dichas consultas (cdo. 99 RGPD). Presentado el proyecto, o la modificación o ampliación, y siempre que no se refiera a actividades de tratamiento en varios Estados miembros, la autoridad de control dictaminará acerca de su conformidad con el RGPD y, en su caso, aprobará dicho proyecto de código, modificación o ampliación, si considera suficientes y adecuadas las garantías ofrecidas, registrándolo y publicándolo a continuación.

Por el contrario, cuando el proyecto, o la modificación o ampliación, se refiera a actividades de tratamiento en varios Estados miembros, la autoridad de control que sea competente en virtud del artículo 55 RGPD lo presentará por el procedimiento mencionado en el artículo 63 RGPD, antes de su aprobación o de la modificación o ampliación, al CEPD, que deberá dictaminar si es conforme con el RGPD o, en la situación indicada en el artículo 40.3 RGPD, si ofrece garantías adecuadas. De ser positivo este dictamen, el CEPD lo presentará a la Comisión, que podrá decidir, mediante actos de ejecución adoptados siguiendo el procedimiento de examen del artículo 93.2 RGPD, que el código de conducta o la modificación o ampliación aprobados y presentados tengan validez general dentro de la Unión, dándole igualmente la publicidad adecuada.

En cuanto a su contenido, los códigos de conducta deberán especificar la aplicación del RGPD respecto de:

a) el tratamiento leal y transparente;
b) los intereses legítimos de los responsables;
c) la recogida de datos personales;
d) la pseudonimización de datos;
e) la información a facilitar al público y a los usuarios;
f) los derechos de los interesados;
g) la información a niños y cómo obtener el consentimiento o tutela de los padres o tutores;
h) la responsabilidad del responsable, privacidad desde el diseño y privacidad por defecto, y medidas de seguridad;

i) las notificaciones de brechas de seguridad;
j) las transferencias internacionales;
k) la resolución de conflictos, sin perjuicio de las actuaciones de la autoridad de control y los juzgados y tribunales; y,
l) los mecanismos de control del cumplimiento del propio código de conducta, sin perjuicio de las competencias de la autoridad de control.

Además, resulta interesante destacar que *ex* artículo 40.3 RGPD, en relación con el artículo 46.2.e) RGPD, los responsables o encargados a los que no se aplica el RGPD en virtud de su artículo 3 podrán adherirse también a códigos de conducta aprobados de conformidad con el procedimiento ya expuesto, a fin de ofrecer garantías adecuadas en el marco de las transferencias de datos personales a terceros países u organizaciones internacionales, permitiendo así la transmisión de datos personales a un tercer país respecto del que no exista una previa decisión de adecuación de conformidad con el artículo 45 RGPD, y sin que en ese caso sea necesario solicitar autorización a una autoridad de control. Eso sí, dichos responsables o encargados deberán asumir compromisos vinculantes y exigibles, por vía contractual o mediante otros instrumentos jurídicamente vinculantes, para aplicar dichas garantías adecuadas, incluidas las relativas a los derechos de los interesados. Sobre este aspecto puede consultarse el capítulo 9 de la presente obra para un análisis más detallado.

La supervisión del cumplimiento de los códigos de conducta se llevará a cabo no solo por la autoridad de control (*ex* arts. 57 y 58 RGPD), sino también (salvo en los casos en que el tratamiento haya sido realizado por autoridades y organismos públicos) por aquellos organismos que, teniendo el nivel adecuado de pericia en relación con el objeto del código, hayan sido acreditados para tal fin por la autoridad competente de conformidad con las reglas establecidas en el artículo 41 RGPD. Para ello, el organismo deberá cumplir, además de los criterios que determine la autoridad de control competente y que apruebe el CEPD (art. 41.3 RGPD en relación con los art. 63 y 64.1.c) RGPD), cuatro requisitos:

a) demostrar, a satisfacción de la autoridad de control competente, su independencia y pericia en relación con el objeto del código;
b) establecer procedimientos que le permitan evaluar la idoneidad para aplicar el código de los responsables y encargados correspondientes, supervisar el cumplimiento de sus disposiciones y examinar periódicamente su aplicación;
c) establecer procedimientos y estructuras para tratar las reclamaciones relativas a infracciones del código o a la manera en que el código haya sido o esté siendo aplicado por un responsable o encargado del tratamiento, y para hacer dichos procedimientos y estructuras transparentes para los interesados y el público; y,
d) demostrar, a satisfacción de la autoridad de control competente, que sus

funciones y cometidos no dan lugar a conflicto de intereses.

En aquellos casos en que estos organismos de supervisión detecten una infracción del código por un responsable o encargado del tratamiento deberán, previa la adopción de las garantías adecuadas, tomar las medidas oportunas para impedir que la infracción se siga cometiendo -puede incluso llegar a suspender o excluir al responsable o encargado-, e informar de ellas y de los motivos que le llevaron a tomarlas a la autoridad de control competente (art. 41.4 RGPD).

Igualmente, dispone el RGPD que la autoridad de control competente revocará la acreditación de un organismo de supervisión si las condiciones de la acreditación no se cumplen o han dejado de cumplirse, o si la actuación de dicho organismo infringe el RGPD.

5.2. Certificaciones

Desconocidas por la Directiva 95/46/CE, el RGPD regula las certificaciones, tal y como sucede con los códigos de conducta, como un mecanismo que *"puede servir de elemento para demostrar el cumplimiento de las obligaciones por parte del responsable"* (cdo. 81 RGPD). Simultáneamente, y con el fin de aumentar la transparencia y el cumplimiento, el RGPD establece la necesidad de fomentar el establecimiento de mecanismos de certificación y sellos y marcas de protección de datos, que permitan a los interesados evaluar con mayor rapidez el nivel de protección de datos de los productos y servicios correspondientes (cdo. 100 RGPD). Por tanto, cumplen también una doble función: prueban el cumplimiento de obligaciones y ayudan a generar confianza.

Regulada por el RGPD como un mecanismo voluntario (art. 42.3 RGPD), la certificación consiste en la obtención de un distintivo que acredita el cumplimiento de las normas establecidas en el propio Reglamento respecto de las operaciones de tratamiento de los responsables y los encargados (art. 42.1 RGPD), así como el cumplimiento de las obligaciones establecidas en materia de protección desde el diseño y protección por defecto (art. 25.3 RGPD)

Esta certificación puede ser expedida por varias entidades.

a) En primer lugar, refiere el RGPD a los organismos de certificación del artículo 43, a los que define como terceros *"que tengan un nivel adecuado de pericia en materia de protección de datos"*. Junto a ello, y para que un organismo de certificación pueda operar como tal, debe reunir una serie de requisitos:
    1. ser independiente (y, por tanto, demostrar la inexistencia de un conflicto de intereses);
    2. ser transparente, respecto del propio proceso de certificación;
    3. haber establecido procedimientos para expedir, revisar y retirar certificaciones;

4. contar con procedimientos para dar respuesta a las reclamaciones que pudieran producirse por infracciones de la certificación.

Estos organismos de certificación serán responsables de la correcta evaluación a efectos de certificación o de retirada de la certificación, sin perjuicio de la responsabilidad del responsable o del encargado del tratamiento en cuanto al cumplimiento del RGPD. La acreditación para poder operar como organismo de certificación se realizará sobre la base de los criterios aprobados por la autoridad de control que sea competente en virtud de los artículos 55 y 56 RGPD, o por el Comité de conformidad con los artículos 63 y 64 RGPD. Igualmente, es posible que esa acreditación se lleve a cabo por el organismo nacional de acreditación designado de conformidad con el Reglamento (CE) 765/2008 del Parlamento Europeo y del Consejo, de 9 de julio de 2008, por el que se establecen los requisitos de acreditación y vigilancia del mercado relativos a la comercialización de los productos y por el que se deroga el Reglamento (CEE) 339/93; con arreglo a la norma EN ISO/IEC 17065/2012 y a los requisitos adicionales que pueda establecer la autoridad de control competente. En el caso concreto de España, este organismo nacional de acreditación es la Entidad Nacional de Acreditación (ENAC), en virtud del Real Decreto 1715/2010, de 17 de diciembre (así lo establece expresamente el artículo 39 del Proyecto de Ley Orgánica de Protección de Datos).

Una vez expedida, la acreditación tendrá validez por un período máximo de cinco años y podrá ser renovada en las mismas condiciones, siempre y cuando el organismo de certificación cumpla los requisitos establecidos en el citado artículo 43 RGPD:

1. responder de la correcta evaluación a efectos de certificación o retirada de la certificación;
2. comunicar a las autoridades de control competentes las razones de la expedición de la certificación solicitada o de su retirada; y
3. mantener los requisitos que fueron necesarios para adquirir la acreditación en primer lugar.

Precisamente, en relación con este último, el artículo 43.7 RGPD permite a la autoridad de control competente o al organismo nacional de acreditación revocar la acreditación a un organismo de certificación si las condiciones de la acreditación no se cumplen o han dejado de cumplirse, o si la actuación de dicho organismo de certificación infringe el RGPD.

b) En segundo lugar, puede expedir la certificación la propia autoridad de control competente, sobre la base de los criterios que ella misma debe aprobar de conformidad con el artículo 58.3.e) y f) RGPD, que le otorga competencia para *"acreditar los organismos de certificación con arreglo al artículo 43"* y para *"expedir certificaciones y aprobar criterios*

de certificación con arreglo al artículo 42, apartado 5".

c) Y, por último, también está legitimado para expedir la certificación el Comité, de conformidad con el artículo 63 RGPD. En este último caso, cuando los criterios sean aprobados por el Comité, podrá darse lugar a una certificación común: el Sello Europeo de Protección de Datos.

La utilización del mecanismo de certificación requiere que los responsables o encargados que sometan su tratamiento al mismo den al organismo de certificación o autoridad de control competente toda la información necesaria para llevar a cabo el procedimiento de certificación, así como acceso a sus actividades de tratamiento (art. 42.6). Concedida la certificación, no quedará limitada la responsabilidad del responsable o encargado del tratamiento en cuanto al cumplimiento del RGPD, y se entenderá sin perjuicio de las funciones y los poderes de las autoridades de control que sean competentes (art. 42.4 RGPD).

De conformidad con el artículo 42.7 RGPD, la certificación se expedirá a un responsable o encargado de tratamiento por un período máximo de tres años y podrá ser renovada en las mismas condiciones, siempre y cuando se sigan cumpliendo los requisitos pertinentes. Asimismo, la certificación será retirada, por los organismos de certificación o la autoridad de control competente, cuando no se cumplan o se hayan dejado de cumplir los requisitos que fue necesario cumplir para su concesión.

BIBLIOGRAFÍA

Ann Cavoukian, "Privacy by design. The Foundational Principles", agosto, 2009. Disponible en: www.privacybydesign.ca.

— "*Privacy by Design* in Law, Policy and Practice. A White Paper for Regulators, Decision-makers and Policy-makers", agosto 2011. Disponible en: www.privacybydesign.ca

Carpio cámara, m: "Seguridad del tratamiento de los datos personales y notificaciones de violaciones de seguridad". En: piñar mañas, j.l., (Dir.): *Reglamento general de protección de datos. Hacia un nuevo modelo de privacidad*, Reus, Madrid, (2016).

Díaz-Romeral Gómez, A., "Los códigos de conducta en el reglamento general de protección de datos", Álvarez Caro, M., Recio Gayo, M. (coords.); y Piñar Mañas, J. L., (dir.), *Reglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad*, Reus, 2016.

Duaso Calés, R., "Los principios de protección de datos desde el diseño y protección de datos por defecto", en Piñar Mañas, J. L., (Dir.) *Reglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad,* Reus, Madrid, 2016, pp. 295-320.

Fernández Sánchez, C. M., y Recio Gayo, M., "Certificación en protección

de datos personales", en Álvarez Caro, M., Recio Gayo, M. (coords.); y Piñar Mañas, J. L., (dir.), *Reglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad*, Reus, 2016.

Guillén Catalán, R., "La vulneración de la protección de datos personales por las redes sociales", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 45, Navarra, 2017.

López Jiménez, D., "La protección de datos de carácter personal en el ámbito de las redes sociales electrónicas: el valor de la autorregulación", *Anuario de la Facultad de Derecho de la Universidad de Alcalá*, núm. 2, Madrid, 2009.

— "Los códigos de conducta. Solución idónea frente a la elevada desprotección de la privacidad en internet", *Revista TELOS (Cuadernos de Comunicación e Innovación)*, núm. 89, Madrid, 2011.

Luca Bolognini; Camila Bistolfi, "Pseudonymization and impacts of Big (personal/anonymous) Data processing in the transition from the Directive 95/46/EC to the new EU General Data Protection Regulation", *Computer Law and Security Review*, núm. 33, 2017, pp. 171-181.

Maluquer de Motes i Bernet, C. J., "Los códigos de conducta como fuente de Derecho", *Derecho privado y Constitución*, Nº 17, 2003.

Millares López, R., "Evaluación de impacto relativa a la protección de datos y consulta previa (Arts. 35 y 36), en López Calvo, J., *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos*, *Adaptado al Proyecto de Ley Orgánica de Protección de Datos de 10 de noviembre de 2017*, Wolters Kluwer, Madrid, 2018, pp. 471-491.

Recio Gayo, M., "Aproximación basada en el riesgo, evaluación de impacto relativa a la protección de datos personales y consulta previa a la autoridad de control", en Piñar Mañas, J. L., (Dir.) *Reglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad,* Reus, Madrid, 2016, pp. 351-366.

Ribagorda garnacho, a: "Las medidas de seguridad en el Reglamento de desarrollo de la Ley Orgánica 15/1999 de protección de datos de carácter personal", en: Troncoso Reigada, a (Dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal,* Aranzadi, Navarra, (2010).

Rubí Navarrete, J., "Códigos de conducta y comercio electrónico", *Informática y derecho: Revista iberoamericana de derecho informático*, Nº 30-31, 1999.

Villarino Marzo, J., "La privacidad desde el diseño en la propuesta de reglamento europeo de protección de datos", *Revista Aranzadi de derecho y nuevas tecnologías,* núm. 32, 2013, pp. 45-68.

Virguri Cordero, J., "Los mecanismos de certificación (códigos de conducta, sellos y marcas)", en Rallo Lombarte, A., y García Mahamut, R. (coords.), *Hacia un nuevo derecho europeo de protección de datos: Towards a new european data protection regime*, Tirant lo Blanch, 2015.

Otras fuentes bibliográficas

Documento de Trabajo 168 "The Future of Privacy Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data", adoptado el 1 de diciembre de 2009, [02356/09/EN].

Documento de Trabajo 248 rev. 01, "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679", adoptado el 4 de abril de 2017, [17/EN].

32nd International Privacy of Data Protection and privacy commissioners, Privacy by design resolution, 27-29 octubre 2010, Jerusalén, Israel.

AEPD, Guía para una Evaluación de Impacto en la Protección de Datos Personales (EIPD), 2014. Accesible en: https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Gui a_EIPD.pdf

Directrices sobre violaciones de seguridad. Guidelines on Personal data breach notification under Regulation 2016/679. Adopted on 3 October 2017 As last Revised and Adopted on 6 February 2018.

Guía del Reglamento General de Protección de Datos para responsables de tratamiento. Agencia Española de Protección de Datos. (2018).

Jurisprudencia

STEDH, I. contra Finlandia, nº 20511/03, de 17 de julio de 2008.