Universidad Internacional de La Rioja

Facultad de Derecho

Grado en Derecho

El Delegado de Protección de Datos Personales

Trabajo fin de estudio presentado por:	Marisa Analía Sarmantano
Tipo de trabajo:	Trabajo Fin de Grado
Directora:	Elena Davara Fernández de Marcos
Fecha:	14 de Septiembre de 2022

Resumen

En el presente trabajo abordaremos el rol e importancia de la figura del Delegado de Protección de Datos Personales, cuáles son sus funciones, obligaciones, responsabilidades y habilidades necesarias como pieza de vital importancia en los Programas de Protección de Datos Personales por parte de las organizaciones y empresas, quienes deben cumplir en forma eficaz y proactiva con una serie de medidas y garantías para proteger los datos personales de las personas, en el marco de un principio que atraviesa toda la normativa, la Responsabilidad Demostrada conocido en su traducción al inglés como «*Accountability*».

Se pretende exponer como este nuevo enfoque conlleva la oportunidad de crear una cultura corporativa en el seno de las organizaciones, una verdadera gestión de datos, donde se inculque el respeto y toma de conciencia sobre el valor que tienen, como se protegen los derechos de los titulares de los datos, su correcta captación, almacenamiento, uso y tratamiento en todos los niveles jerárquicos.

Haremos un breve análisis de las ventajas que trae aparejada la designación del Delegado de Protección de Datos Personales, donde se lo podrá ver como un promovedor de seguridad jurídica, un valor agregado y no un coste para la organización, comportando beneficios tales como lograr una optimización de los productos y servicios ofrecidos, de los recursos en el procesamiento de la información, una definitiva mejora de imagen y como puede redundar en un gran atenuante en la graduación de sanciones frente a vulneraciones a la seguridad de los datos personales.

Palabras clave: Delegado de protección de datos personales, responsabilidad proactiva, régimen sancionador, Reglamento General de Protección de Datos, privacidad, programas de protección.

Abstract

In this paper we will address the role and importance of the figure of the Personal Data Protection Officer. We will explore what are their functions, duties, responsibilities and skills needed to further emphasize the vital role they play in the Personal Data Protection Programs by organizations and companies. This role is a fundamental part as they are who must comply effectively and proactively with a series of measures and guarantees to protect the personal data of individuals, under the principle that runs through all the rules, the Demonstrated Responsibility known in its English translation as «Accountability».

We will expose how this new approach brings the opportunity to create a corporate culture within organizations, real data management where respect and awareness of the value they have is taken into account. We will also dive into how they are protected the rights of data subjects, their correct collection, storage, use and treatment at all hierarchical levels.

We will make a brief analysis of the advantages brought about by the appointment of the Personal Data Protection Delegate. We will show how they can be seen as a promoter of legal security, an added value and not a cost for the organization. While bringing benefits such as achieving an optimization of the products and services offered, the delegate provides resources in the processing of information. This most importantly translates in a definite improvement of image and how it can result in a great mitigation and in a graduation of sanctions against violations to the security of personal data.

Keywords: Personal data protection officer, proactive responsability, sanctions regime, General Regulation of Personal Data Protection, privacy, protection programs.

Índice de contenidos

1. Introducción

El presente trabajo pretende desarrollar el perfil que debe poseer un Delegado de Protección de Datos Personales, quien en adelante denominaremos DPD, cuál es su ámbito de actuación, la posición que ostenta, sus principales funciones y responsabilidades. Que organizaciones o instituciones deben contar con un DPD en el seno de su empresa en el marco 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, en adelante RGPD y de la Ley Orgánica 2/2018 de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, en adelante LOPDPGDD, que garanticen su cumplimiento, en manos de personas capacitadas y especializadas en protección de datos personales.

El RGPD se establece en el ámbito de la Unión Europea, en adelante UE, con el fin de dotar de criterios uniformes y coherentes, que brinden seguridad jurídica, cuyas normas son directamente aplicables en todos los estados miembros de la UE y con plenos efectos jurídicos. Surgió desde la necesidad de adaptarse a las nuevas circunstancias y escenarios, consecuencia de la rápida evolución tecnológica, donde los datos personales, se multiplican y se hacen cada vez más accesibles para todos y además cumplen un rol fundamental para el desarrollo y funcionamiento de los nuevos mercados, del que deriva un ineludible control de su uso y destino.

Su entrada en vigor, supuso la implementación de un sistema de protección de los datos, basado en la prevención, que consagra e impregna en el desarrollo de toda la normativa, con el principio de Responsabilidad Proactiva, y se traduce en el deber por parte de los organismos y empresas, de implementar una serie de técnicas organizativas, para garantizar su cumplimiento, entre ellas se destaca el nombramiento del DPD.

Este principio, significará que el responsable de tratamiento o el encargado de tratamiento de datos, en adelante RT y ET respectivamente, deba no sólo cumplir con toda la normativa, sino también demostrar que *la* cumple y *como* la cumple. «Se trata de un deber de diligencia que

rebasa el puro formalismo y atiende a las actuaciones materialmente emprendidas por el responsable en cumplimiento de sus deberes legales» (GAMERO 2019, p.1).

Esta actitud proactiva permitirá anticiparse y aplicar medidas que eviten caer en incumplimientos. Con ello, se encuadra la contratación del DPD, que se presenta como obligatoria para las empresas públicas y privadas que la ley determine, para facilitar el cumplimiento y garantizar la seguridad en el tratamiento de datos.

Evaluaremos los beneficios de poseer un DPD, al que veremos como valor añadido y no como un coste para las organizaciones. La importancia de que las empresas implanten una cultura corporativa, con un nuevo enfoque, orientado a promover y fomentar la cultura de la protección de datos que atraviese transversalmente todos los niveles jerárquicos.

1.1.Justificación del tema elegido

El esquema implantado por el RGPD trajo un caudal de normas, concebidas con el fin de garantizar la correcta captación, almacenamiento, uso y tratamiento de los datos que reúnen los organismos y empresas.

Se estatuye que tanto el RT como el ET deberán cumplir con los principios relativos a la protección de datos, que deberán ser tratados bajo los principios de licitud, lealtad y transparencia, que su recogida sea limitada al fin y en el tiempo de conservación, la minimización de datos, su exactitud, integridad y confidencialidad, así como ser capaz de demostrarlo, por el principio de responsabilidad proactiva (art. 5 RGPD).

Dentro de este esquema, el rol que debe cumplir el DPD es vital, por ello delimitar su alcance, el perfil y habilidades, funciones, posición y responsabilidad nos ayuda a entender como sirve de engranaje a todo el sistema.

Además de los supuestos donde la designación del DPD es de carácter preceptivo, procuramos resaltar, fuera de esos casos, que una designación voluntaria puede ser conveniente y necesaria cuando así derive del cumplimiento de los principios de la normativa, de los objetivos de la empresa, como evitar costes de una posible violación a la protección de datos personales, así como daños reputacionales que derivarían en pérdida de confianza.

Todas las exigencias impuestas, nos vienen a dar la oportunidad de darle un nuevo enfoque corporativo a las organizaciones, un nuevo reto, que será consolidar una cultura corporativa adecuada, que interiorice la importancia de la protección de datos como un hábito hacia el cumplimiento de las normas.

Si bien, nadie discute la importante y envergadura que contiene el elemento sancionador, y como el temor a posibles condenas en muchos casos es el impulso que tienen las empresas para tomar medidas concretas y así evitar sanciones que pueden alcanzar montos elevados y poner en jaque la continuidad de cualquier pequeña y mediana empresa, éste debería ser un elemento secundario y la prioridad estar puesta en la gestión, poniendo énfasis en la formación, la concientización y puesta en valor, en los controles y en el ejemplo desde el liderazgo, para conservar la confianza de los clientes, que en definitiva es el activo empresarial más valorado.

1.2. Problema y finalidad del trabajo

Centraremos el análisis en delimitar el rol del DPD, evaluar las posibles responsabilidades personales derivadas del ejercicio de su función, en los diferentes escenarios posibles, tanto en el área administrativa, civil y penal, como así también la posición que va adoptando la Jurisprudencia frente a los supuestos grises que se presentan.

Como finalidad intentaremos poner en valor su designación, los beneficios empresariales, tanto económicos como de imagen, más allá de los supuestos en que la ley lo exige, y como propiciante de posibles atenuantes en la responsabilidad de las empresas.

También destacar la importancia que tiene la concientización de la ciudadanía, sobre el poder que tiene sobre sus datos personales, que son considerados oro por las empresas que los manejan, a fin de conocer sus experiencias digitales, hábitos, preferencias y necesidades, que les otorgan claras ventajas competitivas. Por ello, es fundamental que puedan conocer sus derechos y alcance, como herramientas para hacerlos valer y decidir sobre el uso que se hace de sus datos y equilibrar la balanza del poder, a fin de exigir transparencia y seguridad.

Del lado de las empresas, se torna elemental diseñar una estructura basada en el respeto a la regulación, tener la capacidad de transmitir al cliente que sus datos son importantes, en

fidelidad con el cliente, otorgando seguridad y transparencia, a un usuario que tenderá a ser cada vez más exigente, en garantizar su protección con un inconfundible sello ético.

Conforme lo expresado por Miguel A. Abellán, de la consultora especializada en protección de datos Audidat, que dice que cuanto más saben, más denuncian a las empresas que creen han vulnerado sus derechos (DE ZARATE 2022).

1.3.Objetivos

Como objetivos del presente trabajo, se plantea:

- Analizar el perfil, rol, funciones del DPD en el ejercicio de sus funciones.
- Analizar en base a la normativa del RPGD y de la LOPDPGDD que tipo de responsabilidad Civil, Penal y/o Administrativa puede tener el DPD frente a terceros por incumplimientos en la normativa de protección de datos.
- Las sanciones a las que pueden verse afectadas las organizaciones y empresas por incumplimiento a designar el DPD cuando ésta es preceptiva.
- La conveniencia de contar con un DPD independientemente de que su designación se halle prescripta como obligatoria o no por la norma.
- El DPD como factor de graduación a las multas administrativas impuestas a las organizaciones y empresas por responsabilidad frente a filtraciones a seguridad de datos.
- La importancia de generar una conciencia de cumplimiento, una cultura corporativa y de estrategia de datos.
- La importancia de la toma de conciencia de la ciudadanía del valor que tienen sus datos personales.

2. Marco Teórico y Desarrollo

2.1. Protección de los datos personales: La nueva realidad

La Constitución Española de 1978, en adelante CE, garantizó el derecho fundamental a la intimidad personal y familiar (art. 18.1 CE).

El Convenio N° 108 del Consejo de Europa, de 28 de enero de 1981, fue el primer instrumento internacional jurídicamente vinculante, adoptado para la protección de las personas, respeto al tratamiento automatizado de los datos personales.

El Derecho fundamental a la protección de los datos personales fue recogido en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea del año 2010.[1]

Pero es el Tribunal Constitucional, en adelante TC, el que construyó una sólida doctrina que le dio contenido como derecho fundamental al derecho de protección de datos personales (MARTÍNEZ 2019).

Estamos frente a una nueva realidad, compleja y diversa de nuevos desafíos digitales. En un contexto social de globalización, donde la velocidad, el caudal y la trascendencia que tomaron los datos se han incrementado en forma directamente proporcional a la amenaza sobre la privacidad.

La capacidad y rapidez que alcanzan las empresas con los avances tecnológicos para procesar, recopilar y analizar datos de clientes, empleados y proveedores, les permite conocer sus hábitos y preferencias, a una gran escala, y así optimizar los productos y servicios, pudiendo ofrecer un valor añadido frente a sus competidores, lo que expuso la imperiosa necesidad de engendrar un cambio de paradigma con relación a la protección de datos personales.

Así es como el RGPD termina de armonizar y unificar la regulación que tenía cada uno de los estados comunitarios, instaurando un cambio definitivo en la forma de proteger la privacidad, pasando de un modelo de cumplimiento reactivo, a uno basado en la prevención, convirtiéndose en la piedra angular y principal normativa que desarrolla el derecho a la protección de datos personales, con protección constitucional.

Ahora bien, el alcance del derecho a los datos personales no es absoluto, sino que debe guardar proporción con la función que cumplen en la sociedad, en equilibrio con otros

[1] Artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea: «1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. 2. Estos datos se tratará de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación. 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente.»

derechos fundamentales, reconociendo el valor que tienen los datos de las personas en las economías, conforme al principio de proporcionalidad (considerando 4 y 6 RGPD).

2.2. El Principio de Responsabilidad Proactiva

El RGPD vino a imponer un nuevo reto para las empresas, y se basa en dos pilares fundamentales: la responsabilidad proactiva y el enfoque de riesgo, que impregnan el conjunto de la regulación dictada (CARDONA 2019).

La consagración del principio de Responsabilidad Proactiva, atraviesa transversalmente toda la normativa, según la cual el RT y ET deberán diseñar y aplicar medidas técnicas y organizativas que sean adecuadas y apropiadas para garantizar y demostrar que la captación, almacenaje, tratamiento y uso de los datos personales se adapte y cumpla el nuevo plexo normativo.

Pasamos de la cultura del papel a la responsabilidad proactiva, y con ello la necesidad de llevarlo a la práctica, afianzarse en el ejercicio del cumplimiento que realizan diariamente las organizaciones responsables o encargadas de tratamiento y en el ejercicio de los profesionales Delegados de protección de datos.

No debe usarse más la expresión «yo cumplo» o «ya he cumplido», la nueva realidad debe expresarse como «estoy cumpliendo» y puedo acreditarlo (SIMON y BACARIA (coord.) 2020).

A lo largo del RGDP encontramos diversas medidas donde se concreta el principio de responsabilidad proactiva, que brevemente mencionaremos:

1. El análisis de riesgos, que incluyen las fases de su identificación, evaluación y aplicación de medidas de tratamiento de los riesgos.

2. El registro de actividades de tratamiento, donde se recogerá y permitirá identificar el origen y las etapas por las que pasa un proceso de operación de tratamiento, posibilitando el seguimiento y control y a la AEDP verificar la diligencia.

3. Protección de datos desde el diseño (PbD) y por defecto (PDpD). La PbD requiere que los requisitos de privacidad para todo producto o servicio que conlleve tratamiento de datos personales, sea encarado desde las primeras fases de su diseño. Y en la PDpD sólo serán objeto

de tratamiento los datos personales que sean «adecuados, pertinentes y limitados a los necesarios en relación con los fines» (art. 5.1.c) RGPD).

4. Procedimientos que garanticen el ejercicio de los derechos (acceso, rectificación, supresión, limitación, oposición, entre otros) en materia de protección de datos, para facilitar tanto la solicitud como la respuesta frente a estos.

5. Procedimientos para gestionar incidentes de seguridad, ya que, frente a un incidente que afecte los datos personales, será necesario contar con protocolos de actuación, que permitan una rápida y efectiva intervención.

6. Las evaluaciones de impacto en la protección de datos, en adelante EIPD, cuando existan tratamientos concretos que entrañen alto riesgo.

7. Realización de Auditorías para la supervisión.

8. Adhesión a Códigos de Conducta y Certificaciones.

9. Nombramiento del DPD, que desarrollamos a continuación.

2.3. El delegado de protección de datos personales

Si bien la RGPD se encarga de definir el sentido y alcance de los conceptos implicados en la normativa, como datos personales, tratamiento, fichero, responsable de tratamiento, encargado de tratamiento, entre otros, no define al DPD, al que entendemos del análisis y estudio conjunto de los arts. 37, 38 y 39 del RGPD y 34, 35, 36 y 37 de la LOPDGDD, de donde surgen sus principales características y funciones.

La Real Academia Española lo define como la «Persona designada por el responsable y el encargado del tratamiento de datos personales en los casos legalmente previstos a la que compete asesorar a aquellos sobre las obligaciones que les incumben y supervisar el cumplimiento de la normativa en materia de protección de datos» (RAE 2022).

La definición brindada por el Documento relativo a la Evaluación de Impacto de la Comisión Europea sobre la Propuesta del Reglamento, es más precisa, si bien no hace referencia al tipo de formación que debiera ostentar la persona que ejerza la función, la que se traduce del inglés como «aquella persona, responsable en el seno de un responsable o de un encargado del tratamiento, de realizar la supervisión y monitorización, de forma independiente, de la

aplicación interna y de garantizar el respeto a las normas en materia de protección de datos personales, pudiendo ser desempeñado tanto por un empleado interno como por un consultor externo» (COMISION EUROPEA, COMMISION STAFF WORSDKING PAPER 2012, p.3).

El DPD resulta por lo tanto diferenciado del RT y ET, ya que el RT, es el encargado de determinar los fines y los medios del tratamiento, es decir los *para qué* y el *cómo* se van a tratar los datos personales y el ET presta un servicio al RT y sigue sus instrucciones a diferencia del DPD, que es imparcial (DAVARA y DAVARA (Coords.) 2021).

El DPD podrá ser de carácter interno o externo a la organización, es decir, formar parte de la planta de empleados contratados del RT o del ET o bien podrá ser prestador externo mediante contrato de servicios. Lo que deberá estar claro, como veremos más adelante, es que en cualquiera de los casos, aun cuando se encuentre en relación de dependencia, no recibirá instrucciones ni órdenes para el ejercicio de su cargo, ya que se ha configurado que sea una figura independiente. Velará por el cumplimiento del tratamiento de datos dentro de la organización, y asesorará tanto al RT, ET como al personal de la empresa dentro de la materia de protección de datos, además de concientizar y supervisar su cumplimiento.

Es un intermediario entre el RT y ET con los interesados y con la Autoridad de control. También es colaborador con la Autoridad de control, que a nivel comunitario es el Supervisor Europeo de Protección de Datos (SEPD) y en España a nivel estatal es la Agencia Española Datos Personales, en adelante AEDP, existiendo además agencias autonómicas en su ámbito territorial.

2.3.1 Perfil y Habilidades del DPD

Respecto a los requisitos, aptitudes o cualidades personales, perfil profesional, grado de experiencia y estudios que debe poseer una persona para ser DPD, la LOPDPGDD y el RGPD incluyen varias precisiones al respecto, las que se encuentran especialmente recogidos en el art. 37 del RGPD y arts. 34 y 35 de la LOPDPGDD.

El DPD será elegido y designado atendiendo a sus cualidades profesionales, en particular, a su formación y conocimientos especializados en Derecho y la formación en Protección de Datos. También se destaca la práctica en la materia y la capacidad para desempeño de las funciones.

Podrá ser una persona física o jurídica, y respecto a la carga laboral, podrá tener dedicación a tiempo completo o a tiempo parcial, lo que vendrá determinado por el nivel de complejidad, el volumen de los tratamientos, la categoría especial de los datos tratados o riesgos para los derechos y libertades de los interesados.

Siguiendo la normativa citada, podemos reconocer como requisitos para ser DPD, los siguientes:

1. **Especializado en la materia**

El DPD deberá tener un vasto conocimiento y manejo de la legislación nacional, europea e internacional en protección de datos.

Será necesario tener conocimiento de las operaciones concretas de tratamiento que se realicen en el seno de la organización y estar actualizado en la tecnología de seguridad de los datos. El nivel de instrucción y especialización dependerá de la organización de que se trate y de la envergadura de esta, de la cantidad de datos tratados, su complejidad, si existe transferencia internacional de datos, categorías específicas de datos tratados o riesgos para los derechos o libertades de los interesados.

El nivel de especialización en la materia, estará marcado principalmente por las operaciones de tratamiento que se lleven a cabo, así como la protección exigida para los datos personales tratados (considerando 97 del RGPD).

La LOPDPGDD permite establecer mecanismos de certificación voluntarios, a fin de acreditar que el DPD cumple con la cualificación requerida, si bien dicha acreditación no es obligatoria.

Esto es así, ya que tras la discusión parlamentaria sobre este punto se estableció que la acreditación mediante mecanismos de certificación no sea la única forma de demostrar la cualificación para el desempeño de las funciones del DPD (MARTÍNEZ 2019).

Aunque no se exige una titulación específica para adquirir los conocimientos necesarios para el desempeño de sus funciones, lo más recomendado es que tenga formación específica en la materia.

La AEPD, ha establecido un sistema de certificación, que garantiza los conocimientos y las aptitudes de los candidatos a DPD: «Se han identificado, en consecuencia, aquellos conocimientos, habilidades y destrezas necesarias que tiene que poseer la persona a certificar

para llevar a cabo cada una de las funciones propias de la posición de Delegado de Protección de Datos» (AEPD 2019, p.12).

La AEDP exige que: «Para acceder a la fase de evaluación será necesario el cumplimiento de alguno de los siguientes prerrequisitos: 1) Justificar una experiencia profesional de, al menos, cinco años en proyectos y/o actividades y tareas relacionadas con las funciones del DPD. 2) Justificar una experiencia profesional de, al menos, tres años en proyectos y/o actividades y tareas relacionadas con las funciones del DPD, y una formación mínima reconocida de 60 horas en relación con las materias incluidas en el programa del Esquema. 3) Justificar una experiencia profesional de, al menos, dos años en proyectos y/o actividades y tareas relacionadas con las funciones del DPD, y una formación mínima reconocida de 100 horas en relación con las materias incluidas en el programa del Esquema. 4) Justificar una formación mínima reconocida de 180 horas en relación con las materias incluidas en el programa del Esquema» (AEPD 2019, p.15).

Esta formación puede ser online o presencial, contemplando la experiencia adquirida, tanto anterior como posterior a la publicación del RGPD, siempre que sea realizada en el ámbito Nacional y de la Unión Europea. También establece la posibilidad de convalidar hasta un año de experiencia, mediante la justificación de méritos adicionales.

2. Cualidades profesionales

El art. 37.5 del RGPD, en relación a las cualidades profesionales que debe poseer el DPD, determina: « [...] en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos […]»

El RGPD no incluye alusión que permita responder si para asumir la función ha de ser un profesional del ámbito jurídico o es necesario que pertenezca a otros sectores profesionales (DAVARA 2017). Con lo cual, se entiende, que podría ejercer cualquier persona al margen de su titulación, que tenga los conocimientos en la materia, aunque por el tipo de formación requerida, lo lógico sería que sea un abogado o un profesional titulado en Derecho.

Si resultará imprescindible, que tenga sólidos conocimientos y práctica en la regulación nacional, europea e internacional de protección de datos, específicos del sector en el que se mueve, sea privado o en organismos públicos. A ello hay que añadir, conocimientos de los

sistemas de información, competencias digitales, conocer las aplicaciones informáticas y sobre el procesamiento de la información.

El DPD, deberá estar en formación permanente, para poder adaptarse rápidamente con los cambios tecnológicos y la innovación.

Con respecto a las *strong skills* necesarias deberá poseer «grado universitario más doctorado o máster, certificaciones reconocidas, inglés alto, experiencia en protección de datos y conocimientos especializados en derecho y conocimiento TIC» (SARACIBAR 2017, p.62).

En el ámbito de las Administraciones públicas deberán tener formación en la normativa y procedimientos administrativos.

3. Capacidad para su desempeño

Entre las habilidades personales y siguiendo la doctrina, se valoran «proactividad, creatividad, asertividad, visión global, capacidad de impacto e influencia, análisis, planificación, formación continua, trabajo en equipo, accesibilidad, transversalidad, empatía y habilidades de comunicación» (SARACIBAR 2017, p. 62).

El DPD deberá estar comprometido con la cultura de integridad, poseer valores éticos y actuar con honestidad. Estos requerimientos vienen dados por su función vinculada al manejo de datos, recurso valioso y directamente relacionado a la libertad, seguridad y dignidad de las personas, que deberán ser tratados de forma lícita, transparente y ética. «Privacidad, seguridad y ética son componentes imprescindibles de una misma ecuación» (DAVARA 2021, p.1).

De esta forma, para cumplir el rol y las funciones del DPD, será esencial contar con el conocimiento y la práctica, así como la actualización constante. Deberá tener sólidos conocimientos de la legislación, estar especializado en protección de datos y privacidad, contar con formación en tecnologías y de desarrollo de negocios, con las particularidades del ámbito en el que se desempeña.

En definitiva el perfil del DPD será más o menos exigente en función del tipo y envergadura del tratamiento de datos que desarrolle cada empresa.

Por todas las funciones e implicancias que atraviesa, el DPD es una figura muy compleja, multidisciplinar que ocupa un rol activo en la vida y organización de una empresa, es por ello

que debe ser un profesional preparado en función de las particularidades del sector en que actúa, empapándose de su contexto e impregnando a toda la organización y a los procesos de los principios de protección de datos.

2.3.2. Posición del Delegado de Protección de Datos

La posición que ocupa el DPD en el seno de la Organización o empresa, viene delimitado por los Arts. 37 y 38 del RGPD y 36 y 37 de la LOPDPGDD, entre los que se encuentran:

1. Participación necesaria

El DPD deberá intervenir en tiempo oportuno y su participación será adecuada, en todas las cuestiones derivadas a la protección de datos personales.

Significa que el DPD deberá estar implicado desde los inicios de toda materia que esté relacionada con la protección de datos y en todas las áreas que tengan actividades de tratamiento de datos.

Esta intervención temprana garantizará el efectivo cumplimiento del RGPD, y del principio de proactividad, que implicará: Planificar, Hacer, Verificar y Actuar, conocido como ciclo PDCA, metodología incorporada por los estándares internacionales de la International Organization for Standartization, más conocido como normas ISO, referentes en planificación, acción y monitorización en cumplimiento normativo.

El RT y el ET, estarán obligados a darle participación en esos términos: «Se invita al DPD a participar con regularidad en reuniones con los cuadros directivos altos y medios. Se recomienda que esté presente cuando se toman decisiones con implicaciones para la protección de datos. Toda la información pertinente debe transmitirse al DPD a su debido tiempo con el fin de que pueda prestar un asesoramiento adecuado. La opinión del DPD se tiene siempre debidamente en cuenta. En caso de desacuerdo, el Grupo de Trabajo recomienda, como buena práctica, documentar los motivos por los que no se sigue el consejo del DPD. Se consulta al DPD con prontitud una vez que se haya producido una violación de la seguridad de los datos o cualquier otro incidente» (Article 29 Working Party, 2016, p.15 en adelante GT29).

2. Recursos Necesarios

El RT y el ET deberán apoyar al DPD para el desempeño y logro de las funciones inherentes a su cargo, siendo imprescindible para su sostén, la facilitación de los recursos necesarios, tanto económicos, como así también garantizar el acceso efectivo a los datos personales y a las operaciones de tratamiento.

Será fundamental dotarlo de un presupuesto suficiente y acorde al ejercicio de su función, tanto para la obtención de servicios, medios tecnológicos, humanos, en formación y cualquier otro recurso necesario para el correcto funcionamiento de su plan de trabajo. La falta de recursos para el desempeño de su función, conllevará al fracaso del DPD por pérdida de efectividad.

Este elemento se convierte en un requisito imprescindible para que goce de la autonomía e independencia que debe de poseer. A mayor complejidad o sensibilidad de las operaciones de tratamiento, mayores serán los recursos a asignársele.

3. Reporte a la Dirección

El DPD es clave en la rendición de cuentas, ya que se establece que rinde cuentas directamente al más alto nivel jerárquico, teniendo identificado un rol prioritario y estratégico dentro del funcionamiento de la organización o empresa. Ahora bien, para el éxito y eficacia en las funciones del DPD, será esencial que desde los altos cargos de la empresa se cree y fomente una cultura de protección de datos.

Y para ello es fundamental el rol y apoyo del líder conocido como «*Tone from de top»*, que se manifiesta desde el proceso de contratación, en la adopción de normas de conducta internas, siendo visible en la inversión y los recursos dispuestos, a nivel de estructura, de políticas y procedimientos, el entrenamiento, la comunicación y los controles internos. Pero por sobre todo desde el ejemplo y la bajada de tono de los que cumplen un rol fundamental en la empresa y en la puesta en valor de la cultura de protección de datos personales.

El GT29 recomienda el apoyo activo al DPD por parte de la alta dirección, tiempo suficiente para que el DPD cumpla con sus funciones, apoyo adecuado en cuanto a recursos financieros, infraestructura (locales, instalaciones, equipos) y personal según se requiera, comunicación oficial de la designación del DPD a toda la plantilla, acceso a otros servicios dentro de la organización de modo que los DPD puedan recibir apoyo esencial, datos e información de dichos servicios, formación continua (GT29 2016).

4. Independencia

También es primordial dotarlo de independencia para el ejercicio de su labor, brindando un marco de actuación para el DPD en el que pueda ejercer sus funciones con un manto de protección, libre de injerencias e instrucciones, tanto sobre cómo debe orientar su trabajo o como debe proceder y sin que pueda ser sancionado o despedido por ello, salvo que incurriera en dolo o negligencia grave.

«Asimismo, la empresa garantizará que el delegado de protección de datos goce de total libertad, autonomía e independencia en el ejercicio de sus funciones garantizando que no recibirá ninguna instrucción en lo que respecta al desempeño de las mismas y estará respaldado por la organización en el desempeño de las funciones, quien le invitará a participar con regularidad en reuniones con los cuadros directivos altos y medios, a fin de asegurar su presencia en la toma de decisiones relevantes relacionadas con la protección de los datos de carácter personal, gozando en todo momento la opinión del delegado de protección de datos de la consideración debida» (MIGUEL 2019, p. 53).

Estimamos necesario para garantizar la independencia del DPD, el establecimiento y sostenimiento en forma conjunta y simultánea todas las condiciones; que no reciba órdenes respecto al desempeño del cargo atribuido, que sea dotado de los medios materiales y personales necesarios para cumplir sus funciones, la imposibilidad de destitución o sanción por parte del RT o ET por el desempeño de su función y rendición de cuentas directamente a la Alta Dirección de la empresa, en un nivel elevado de gestión.

5. Conflicto de intereses

Otro elemento importante tiene que ver con la necesidad de que el DPD no posea conflicto de intereses, si bien no será necesario que tenga dedicación exclusiva en su función pudiendo desarrollar otros cometidos.

Se deberá analizar, en caso de tener a la misma persona frente al cargo de DPD y otros roles adicionales dentro de la organización, que esa concurrencia no derive en un conflicto de intereses. El conflicto de intereses está estrechamente vinculado con la independencia del DPD. Por ello sería incompatible, ejercer conjuntamente con el cargo de director general, director financiero, de operaciones, jefe de recursos humanos o de TI, por darse especial potencial conflicto de intereses.

«Esto supone, en especial, que el DPD, no puede ocupar un cargo en la organización que le lleve a determinar los fines y medios del tratamiento de datos personales» (GT29 2016, p.26).

También es importante recordar que la dependencia económica y ya sea que se desempeñe dentro de la plantilla de la empresa o como contrato de servicios, no sea un impedimento para su desempeño imparcial.

Romero recomienda, siguiendo a Sonia Martín, que la mejor manera de evitar conflictos de intereses, es que las compañías externalicen el servicio en empresas especializadas en el sector de la protección de datos, principalmente las pequeñas y medianas empresas (ROMERO 2020).

Resulta oportuno recordar como la Autoridad de Protección de Datos Belga, el 28 de abril de 2020, impuso una sanción de 50.000 euros por el incumplimiento de una compañía de evitar un conflicto de intereses previsto en el artículo 38 del RGPD (PWC TAX&LEGAL SERVICES 2020).

6. Accesibilidad

También se requiere que el DPD sea accesible y fácilmente contactable por cualquier interesado en el ejercicio de sus derechos y en cuestiones relativas al tratamiento de sus datos personales.

Se «Recomienda que el DPD se encuentre en la Unión Europea, con independencia de si el responsable o el encargado del tratamiento está establecido en ella» (GT29 2016, p.12).

Resulta imprescindible garantizar que cualquier interesado tenga vía de comunicación expedita y rápida para el ejercicio de sus derechos, la debida publicidad de los datos de contacto del DPD, así como su comunicación a la autoridad de control a fin de que pueda ejercer la intermediación entre ambas (art. 37.7 RGPD).

Asegurar su accesibilidad posibilita que cualquier persona que sienta vulnerado sus derechos en materia de protección de datos, podrá reclamar directamente ante el DPD de la entidad que ha violado sus derechos, con carácter previo a su reclamación ante la autoridad de protección de datos.

Paralelamente el DPD deberá guardar secreto o la confidencialidad en lo que respecta al desempeño de sus funciones, lo que garantiza la operatividad del punto anterior, generando

una mayor predisposición e interés en entablar reclamos por violaciones en el tratamiento de sus datos personales.

Todos los elementos analizados permiten darle al DPD una posición de plena autonomía, que viene asegurada por el RGDP para garantizar sus objetivos, lo que debería tener como resultado lógico y esperable que cada entidad o empresa posea un DPD genuino, verdadero, formado y con la experiencia necesaria para la complejidad y cantidad de datos que se traten.

Ahora bien, para que un DPD pueda desplegar sus funciones en forma efectiva, sin recibir instrucciones y dar opinión sin coacción alguna, con los recursos necesarios para ejercer sus funciones, se torna necesario que la organización, de arriba hacia abajo, este impregnada de la importancia y respeto por la protección de datos personales, con una cultura de cumplimiento y en protección de datos desde los cargos directivos, con un enfoque corporativo, desde el ejemplo, interiorizando el hábito de cumplimiento de protección de datos.

2.3.3. Cuando es obligatorio contratar un DPD

Podemos clasificar la designación del DPD como preceptiva, por así exigirlo la norma o que su designación sea voluntaria, por considerarlo conveniente o necesario para cumplir con la normativa en protección de datos de la organización.

El RGPD establece en su art. 37 cuando el RT o ET debe proceder a su designación:

1. Cuando el tratamiento lo lleve a cabo una autoridad u organismo público, salvo los tribunales cuando actúen en ejercicio de la función judicial.

Autoridad u organismo público comprende la Administración Central del Estado, la Administración de las Comunidades Autónomas, las Entidades que integran la Administración Local y el sector público institucional (RODRÍGUEZ 2019).

Se recomienda que también las organizaciones privadas que llevan a cabo o ejercen función pública designen DPD (GT29 2016).

2. Cuando las actividades principales del RT o ET sean operaciones de tratamiento, que por su naturaleza, alcance y/o fines, requiera de una observación habitual y sistemática de interesados a gran escala.

Por actividad principal se entiende aquellas operaciones imprescindibles para el desarrollo de la actividad del tratamiento para la consecución de sus fines (GONZALEZ 2018).

Para poder determinar cuando estamos frente a gran escala, se deben ponderar los siguientes factores: número de interesados afectados por el tratamiento, alcance geográfico, volumen de datos personales y duración y permanencia de la actividad de tratamiento de los datos personales (GT29 2016).

Habitual se refiere a continuo, por períodos concretos de tiempo, periódico, constante. Y por sistemático, se entiende que se lleva a cabo de acuerdo a un sistema concreto, preestablecido, organizado y metódico, que responde a un plan general y estrategia de recogida (GT29 2016).

3. Cuando consistan en tratamiento a gran escala de categorías especiales de datos personales conforme el art. 9 y de datos de condenas e infracciones penales del art. 10 (art. 37.1 RGPD).

4. Cuando así lo exija el Derecho de la Unión o de los Estados miembros (art. 37.4 RGDP).

Luego la LOPDPGDD en una larga y diversa lista de supuestos, establece concretamente que entidades deberán contar con un DPD en forma obligatoria, entre las que se encuentran los colegios profesionales y sus consejos generales, los centros docentes que ofrezcan enseñanzas en cualquiera de los niveles establecidos en la legislación reguladora del derecho a la educación, así como las Universidades públicas y privadas, los establecimientos financieros de crédito, las empresas de servicios de inversión, reguladas por la legislación del Mercado de Valores, los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes, las empresas de seguridad privada, las federaciones deportivas cuando traten datos de menores de edad, entre otros muchos obligados (art. 34.1 LOPDPGDD).

En cualquiera de los supuestos, se podrá contar con un solo DPD, en el caso de las empresas privadas, si ellas conforman un grupo empresarial siempre que sea fácilmente accesible desde cada establecimiento, y cuando se trate de una autoridad u organismo público, si la estructura organizativa y el tamaño se lo permiten.

La enumeración de los casos comprendidos que efectúa la LOPDGDD, se establece como obligatoria para el cumplimiento de la normativa, pero no es exhaustiva, ya que la no inclusión de otros supuestos en su listado, no significará falta de conveniencia en su designación voluntaria, como veremos en el siguiente apartado.

Formalidades de la designación

La entidad responsable o encargada del tratamiento tiene la obligación de comunicar a la autoridad de control en un plazo de 10 días, toda designación, nombramiento o cese de DPD y también deberá publicitar su existencia a través de medios electrónicos.

En caso de designárselo de manera voluntaria, quedará sometido en su totalidad al cumplimiento del RGPD, tal como si fuera obligatorio.

El RT o ET publicará los datos de contacto del DPD y la AEDP mantendrá una lista actualizada y pública de los DPD, a fin de hacer efectiva la accesibilidad directa de cualquier titular de algún derecho vulnerado frente al DPD.

Respecto a los datos que se publican, si bien no hay precisiones al respecto, se entiende que son los necesarios, tales como correo electrónico, teléfono, formulario web y/o cualquier medio que facilite el contacto con el DPD.

2.3.4 Cuando es conveniente contratar un DPD

En este apartado, pretendemos demostrar, que aún en los casos en los que no sea obligatorio designar un DPD en el seno de la organización, resultará recomendable contar con esta figura.

Como primera premisa, conviene precisar que fuera de los casos establecidos como obligatorios, no existe concreción legal, de que casos convendría designar un DPD, pero si podremos afirmar que sería conveniente su designación voluntaria por parte de los ER y ET cuando así resulte del cumplimiento de los principios de la normativa, motivados por el cumplimiento de la responsabilidad proactiva.

«A menos que resulte obvio que a una organización no se le requiere la designación de un DPD, el Grupo de Trabajo del artículo 29 recomienda que los responsables y encargados del tratamiento documenten el análisis interno realizado para determinar si debe nombrarse o no un DPD, a fin de poder demostrar que se han tenido en cuenta debidamente los factores pertinentes» (GT29 2016, p.6).

«Teniendo en cuenta 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, el responsable y el encargado

del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo […]» (art. 32.1 RGPD).

Encontramos algunos supuestos, que sin ánimo de ser exhaustivos, tornan conveniente la designación voluntaria del DPD, ya sea en vistas del cumplimiento de la responsabilidad proactiva, como por razones de índole económica, cultural, social o de imagen:

1. La normativa establece que cuando sea probable que un tipo de tratamiento entrañe un alto riesgo para los derechos y libertades de las personas, se realizará EIPD (art. 35.1 RGPD) donde el DPD cumple una función clave tanto en la realización y asesoramiento, como en la posterior supervisión de su aplicación (art. 39.1.c), considerando por lo tanto en estos casos necesaria su designación voluntaria.

Es por el rol que juega el DPD en la gestión de procesos críticos, el asesoramiento en la realización de evaluaciones de impacto, la supervisión de los registros de actividades de tratamiento, la gestión de las transferencias internacionales de datos y su gestión en las reclamaciones y brechas de seguridad (SIMON 2018).

De esta manera, una correspondiente EIPD, vendrá determinado por el nivel de complejidad, el volumen de los tratamientos, la categoría especial de los datos tratados o riesgos para los derechos y libertades de los interesados, que permitirá determinar el nivel de riesgo y con ello también la mayor o menor carga laboral, volumen de trabajo y dedicación que tendrá el DPD.

2. Cuando se realicen actividades de tratamiento de datos por procedimientos automatizados, ya que ellos entrañan el riesgo de vulnerar fácilmente los derechos y las libertades de las personas y lo lógico y esperable es que efectúen tratamiento a gran escala, sea por el volumen de datos tratados, número de interesados afectados, como por la duración de la actividad de tratamiento de datos, entre otros, que haría necesaria y conveniente la contratación de un DPD para cumplir con la normativa en materia de protección de datos.

3. Cuando una empresa quiera tomar participación y adquirir competitividad en el mercado, con trascendencia a nivel nacional, europeo e internacional, con un volumen significativo de clientes, deberá adaptarse al nuevo mercado digital y con ello a las posibles consecuencias que ello puede significar, como son los frecuentes ciberataques a los que se ven expuestas.

En lo que va del año se produjeron grandes ataques a compañías, como Facebook, Mercado Libre, Globant, Banco Galicia, Banco Provincia, DHL, BNP, entre otros, por lo que es importante se tomen medidas de prevención y de respuesta frente a los incidentes. Una encuesta realizada a 642 ejecutivos de América, arrojó entre sus datos que el 83% de las compañías sufrió un ciberataque en el último año, el 58% sufrió pérdidas económicas directas y el 20% sufrió daños reputacionales (KPMG 2022).

No obstante, no será de igual magnitud, para RT o ET que tengan tratamiento de datos de menor escala, que las que hagan tratamiento masivo de datos. « […] las empresas y organizaciones deben comprender los escenarios de riesgo que crean para las personas cuando procesan sus datos personales y hacer un esfuerzo conceptual de planificación e implementación para mitigar esos riesgos» (SIMON *et al.* (coords.) 2020, p. 29).

El DPD será clave y ayuda indispensable en la gestión de brechas de seguridad. Si la organización sufre una violación de la seguridad de los datos personales, el DPD le permitirá actuar de forma rápida a la hora de paliar los efectos de la filtración o vulneración de la seguridad (GESDATA CONSULTING 2021).

4. Desde la vigencia del RGPD, las cuantías y empresas involucradas en sanciones han ido aumentando considerablemente con los años. Así en 2020 las multas ascendieron a los 8 millones de euros y en 2021 a los 35 millones de euros (DE ZARATE 2022).

Recientemente, en mayo de este 2022, la AEDP sancionó a Google por 10 millones de euros y a Vodafone España por 3,9 millones de euros por vulnerar la ley. Con esto se prevé que las cifras del año 2022 sean más elevadas en relación con el año anterior.

Para confirmar que estamos frente a una tendencia alcista en la actividad sancionadora de las autoridades de protección de datos, se destaca la reciente multa impuesta a Instagram por vulneración al RGPD, de setiembre de 2022, que asciende a 405 millones de euros por falla en la protección de datos de menores de edad, impuesta por la Comisión de Protección de Datos de Irlanda (EL MUNDO 2022).

Si prejuicio de que esto no será igual para todas las organizaciones y empresas. La medida y alcance de las diligencias que se deberán realizar, que se traduce en una mayor o menor proactividad, viene dada por el factor riesgo, pero contratar un DPD, permitirá enmarcar la empresa en el cumplimiento de los requisitos, y adoptar una estrategia de datos «*Data Driven*

Company», lo que debería poseer cualquier organización que maneje datos personales, y le permitirá ahorrar dinero gracias a las multas que se evitaron, las contingencias que fueron previstas, resolución de ineficiencias internas y donde tendrá el plus de contar con una empresa más sólida.

Además como veremos en otro apartado, la AEDP podría considerar un atenuante de responsabilidad contar con un DPD.

5. Contratar un DPD en el seno empresarial, demuestra compromiso social y respeto con los derechos y libertades de los ciudadanos, al encuadrarse y fomentar una cultura de cumplimiento corporativa.

Poner en la agenda un sistema de gestión de protección de datos personales, puede repuntar también en una ventaja competitiva, donde la gestión de privacidad de datos y la transparencia en su tratamiento, son vistas con buenos ojos por los clientes, fortaleciendo la reputación de la empresa. «Los derechos de la persona afectada deben estar protegidos para evitar daños a la reputación u otras consecuencias negativa» (Considerando (100) Directiva (UE) 2019/1937).

Se destaca que la designación del DPD mejora la imagen corporativa, proyecta valores de compromiso, transparencia y ética profesional. También favorece la creación de una cultura de privacidad. El Delegado de Protección de Datos ayuda a difundir la cultura de respeto a la privacidad dentro de la Organización. Es una figura fundamental para planificar e introducir la Protección de Datos desde el Diseño para realizar acciones y campañas para clientes (GESDATA CONSULTING 2021).

La Asociación Francesa de Corresponsales de Protección de Datos Personales, en adelante AFCDP, establece una lista de buenas razones para nombrar un DPD, entre las que se destacan:

1. Reduce el riesgo legal.

2. Permite implementar el procesamiento de datos con mayor rapidez.

3. Mejora la imagen.

4. Promueve la implementación del enfoque de calidad para la gestión de la información.

5. Mejora la política de seguridad de las tecnologías de la información, en adelante TI.

6. Reduce los costos de procesamiento de información.

7. Reduce los costes de gestión de clientes.

8. Mejora la valoración de los activos de la información (AFCDP 2022).

Para ir concluyendo, cada responsable deberá medir, si en el seno de su empresa, los tratamientos de datos que realiza implican un riesgo elevado o no a los datos personales, que determine el tipo o tipos de tratamiento que realiza, su naturaleza, cantidad de personas afectadas, todo lo cual será esencial para ponderar las diferentes variables y su consiguiente riesgo.

Nos atrevemos a afirmar que la sola presencia del DPD, aún en las organizaciones donde el tratamiento de datos sea de menor entidad, será de enorme utilidad para hacer frente a la exigencia de proactividad, dotará de garantías a la sociedad en su conjunto de que está promoviendo la seguridad jurídica, siendo un buen puente para fortalecer los lazos con consumidores, usuarios y con la sociedad en general, generando credibilidad, confianza y compromiso.

Un DPD resultará un bien intangible para la organización, un sello distintivo de calidad, que va a redundar en definitiva en beneficios reputacionales y de crecimiento económico, que más que en términos de costos, deberá ser erigido a nivel inversión.

2.3.5. Funciones del Delegado de Protección de datos

Las funciones del DPD son múltiples y variables, se encuentran reguladas de la conjunción del art. 39.1 del RGPD y de los arts. 36 y 37 de la LOPDGDD.

Siguiendo la clasificación del Manual del DPD, vamos a delimitar sus funciones en cinco grandes grupos: 1. Organizativas, 2. Supervisión, 3. Consultivas, 4. Cooperación y consulta a la AEDP, 5. Información y sensibilización (AEPD 2019).

Más allá de esta clasificación general, hay que destacar que cada DPD, tendrá matices y funciones diferenciadas, que implicará también conocimientos específicos de acuerdo a la rama o actividad en la que se desarrolle. No es lo mismo para un DPD, desempeñar funciones en entidades públicas o el ámbito empresarial, en universidades, en el sector de la salud, farmacéutico, financiero o asegurador, en el marketing digital, etc., donde cada campo tiene su especificidad.

Deberá tener un conocimiento cabal de la organización y distribución interna, las funciones y líneas de responsabilidad relativas al tratamiento de datos personales, los acuerdos y vínculos con organizaciones externas y el marco legal aplicable a dicha organización.

1. Funciones Organizativas

El DPD deberá crear y mantener un registro de operaciones de tratamiento de datos personales, donde se indique cada operación, el objeto, datos personales, receptores, categoría de interesados y el responsable. De esta manera el RT garantiza el cumplimiento del principio de responsabilidad corporativa exigido por la norma y también permitirá la supervisión por la autoridad de las actividades de tratamiento que realiza.

Deberá revisar las operaciones de tratamiento de datos personales registradas a fin de comprobar que se ajustan al RGPD.

Deberá evaluar los riesgos de diferente probabilidad y grados de gravedad para los derechos y libertades de las personas.

Deberá gestionar las operaciones que puedan tener "alto riesgo", gestionando una EIPD. También será obligatorio realizar un EIPD cuando exista toma de decisiones basadas en perfiles automatizados, tratamiento a gran escala de datos sensibles o supervisión a gran escala de un área accesible al público (art. 35.3 RGPD).

Su participación en los ejercicios de EIPD, le incumbe en todo momento del proceso, desde su asesoramiento sobre: la necesidad de llevarla a cabo, las personas que intervendrán en la evaluación, la metodología que se seguirá e incluso comprobar si le evaluación se realizó correctamente y que se garantizan los derechos de privacidad.

2. Funciones de Supervisión

La función de supervisar el cumplimiento de la organización al RGPD es continua, lo que conlleva revisar y repetir las funciones organizativas mencionadas en el punto anterior, principalmente cuando haya modificación de operaciones de tratamiento, facilitando futuros ajustes o se implanten nuevas.

El DPD deberá gestionar las violaciones a la seguridad de datos personales. Como así también deberá notificar a la AEDP y al interesado, en caso de que se produzca una violación que pueda poner en riesgo los derechos y libertades de las personas.

Podrá investigar, sea por su propia iniciativa o petición de la organización, así como de cualquier persona, sobre asuntos que estén relacionados con sus funciones, debiendo informar los resultados de dicha investigación.

3. Funciones Consultivas

Tiene a su cargo el asesoramiento respecto de las obligaciones derivadas de protección de datos, tanto al RT, al ET como al personal que tenga acceso al tratamiento de datos. Acerca de la evaluación de impacto relativa a la protección de datos, podrá realizar recomendaciones para la mejora y actualización de políticas y prácticas de protección de datos de la organización. Puede ser consultado tanto por la dirección como por el personal o personas que tengan responsabilidades de tratamiento.

Debe fomentar e implicarse la PpD y PDpD. Con esto queremos decir que la protección de datos se debe abordar desde las fases iniciales de la planificación de los sistemas de tratamiento, la seguridad de principio a fin y que los datos deben quedar protegidos automáticamente en el sistema de TI.

Debe asesorar y supervisar el cumplimiento normativo de las políticas de protección de datos vigentes, también tendrá que revisar los documentos y contratos, recomendar las modificaciones necesarias a fin de ajustarlos a todos los requerimientos legales.

También podrá recomendar la implementación de códigos de conducta así como la obtención de certificaciones de protección de datos por parte de su organización.

4. Nexo de contacto

Actúa como intermediario, entre la autoridad y la organización, ejerce como punto de contacto para cualquier cuestión de tratamiento de datos, como la realización de consulta previa por parte del RT o del ET antes de proceder al tratamiento, cuando de la EIPD surja que el tratamiento exista un alto riesgo si no se toman medidas de mitigación, prevista en el art. 36 del RGPD, así como consultas de cualquier otro tema.

El DPD es cooperador de la autoridad de control, respondiendo a las solicitudes que se le ejecuten, cuando se requiera información o para facilitar el acceso a documentos o información requerida. También podrá dirigirse ante la autoridad de control para asesorarse y evacuar consultas.

También es facilitador con el interesado o afectado, gestiona y es canal de recepción de las peticiones sobre protección de datos personales y denuncias de cualquier afectado, quien además de su derecho a reclamar formalmente ante la AEPD, podrá ponerse en contacto directamente con el DPD respecto a cualquier cuestión relativa al tratamiento de sus datos personales, del ejercicio de sus derechos, principalmente los de acceso, rectificación, supresión, limitación y portabilidad de los datos.

De igual manera, si un afectado reclama ante la AEPD, esta dará intervención al DPD, quien deberá atender el reclamo y responder en el plazo de un mes. Caso contrario el procedimiento proseguirá ante la AEPD.

En las relaciones laborales, actúa como nexo entre el personal y sus empleadores, como interlocutor a los efectos de tomar conocimiento de eventualidades.

5. Funciones de Información y Sensibilización

La función de información y concientización, se debe desarrollar tanto a nivel interno, estableciendo los programas de capacitación y concientización del personal, entre otras funciones, como a nivel externo, informando al interesado cuando se recojan sus datos personales, como en la página web de la empresa, donde se deberá trabajar en la transparencia sobre los fines, tratamiento, receptores de datos y si existe transferencia a terceros países, datos del DPD y la forma que pueden ejercer sus derechos.

El cumplimiento de la normativa de protección de datos debe de realizarse de una manera integral, en la que todos los empleados estén implicados en el cumplimiento, por ello es que también se le encomienda la concienciación y formación del personal, como también su participación de las auditorías correspondientes.

2.3.6. Responsabilidad del Delegado de Protección de Datos

El régimen sancionador previsto en el RGPD y la LOPDGDD, se aplica al RT y también el ET, quienes asumen las responsabilidades derivadas por el inadecuado tratamiento de datos personales.

El DPD queda expresamente excluido de las responsabilidades impuestas por las normas de protección de datos (art. 70.2 LOPDGDD).

Sus funciones son de apoyo y asesoramiento, no toma las decisiones, si bien lo lógico es que los responsables actúen conforme lo asesorado por el DPD.

Es decir, que como principio general, el DPD no sería responsable en forma personal por cualquier incumplimiento a las normas de protección de datos personales, si bien en el debate parlamentario algunas enmiendas planteaban su inclusión, todas fueron rechazadas (MARTÍNEZ 2019).

Ahora bien, sentado el principio, habrá que matizarlo con los diferentes escenarios, donde podrían caberle eventualmente al DPD responsabilidades civiles, penales y administrativas y habrá que tenerlas en cuenta:

Responsabilidad Civil

El DPD no será civilmente responsable, siempre y cuando su obrar sea conforme y en ejercicio de sus funciones y al trabajo encomendado.

Cuando actúe fuera de esos límites, se le podrá imputar responsabilidad civil, con la salvedad de que la acción contra él no será directa, el interesado deberá dirigir su acción de responsabilidad contra el RT o ET, y estos podrán ejercer acciones de repetición por la cuantía de daños y perjuicios causados por su negligente actuación, siendo además carga de la prueba del RT o ET que a causa de la negligente actuación del DPD, se provocó el resultado lesivo.

Responsabilidad Penal

El DPD si será penalmente responsable en caso de incurrir en un ilícito tipificado penalmente y con ello, también cabe la extensión de responsabilidad penal hacia las Personas Jurídicas: «No obstante, el RT y el ET deben tener presente el régimen de responsabilidad penal de las personar jurídicas, que puede afectarles en caso de que se acredite la falta de debido control por parte de la dirección de los empleados que intervienen en el tratamiento» (VELAZQUEZ 2017, p.58).

Cuando el delito penal surgiere en virtud de un obrar omisivo de sus funciones, la Doctrina y Jurisprudencia, no han sido ajenas al debate sobre la posible responsabilidad penal del DPD, y han sentado los presupuestos para que se configure el mismo: «Sin embargo, el hecho de que el delegado de protección de datos tuviera transferida la posición de garante no es suficiente para que le sea exigible responsabilidad penal, sino que además es necesario que de la omisión de sus funciones de garantía haya facilitado o, al menos, posibilitado la perpetración del ilícito penal. En este sentido se pronuncia igualmente el Tribunal Supremo en diversas sentencias, como serían la 19/1998 de 12 de enero, la 221/2003 de 14 de febrero,

etc.), cuando dice: "cuando la omisión del deber de actuar del garante haya contribuido, en una causalidad hipotética, a facilitar o favorecer la acusación de un resultado propio de un delito de acción o comisión y que podría haberse evitado o dificultado si hubiera actuado como le exigía su posición de garante"» (MIGUEL 2019, p. 54).

«La jurisprudencia de esta Sala, si bien ha reconocido expresamente que la admisibilidad de una participación omisiva es de difícil declaración, ha aceptado ésta, asociando su concurrencia a la de los elementos propios del art. 11 del CP , entre ellos, que el omitente ocupe una posición de garante (STS 1273/2004, 2 de noviembre). De ahí que sea posible incluso en los delitos de acción, cuando la omisión del deber de actuar del garante haya contribuido, en una causalidad hipotética, a facilitar o favorecer la causación de un resultado propio de un delito de acción o comisión y que podría haberse evitado o dificultado si hubiera actuado como le exigía su posición de garante (cfr. SSTS 19/1998, 12 de enero, 67/1998, 19 de enero, 221/2003, 14 de febrero)» (STS 797/2010).

«La jurisprudencia de esta Sala, en relación con la complicidad omisiva impone la concurrencia de los siguientes requisitos: a) un presupuesto objetivo, esto es, el favorecimiento de la ejecución; b) un presupuesto subjetivo consistente en la voluntad de facilitar la ejecución; y c) un presupuesto normativo, consistente en la infracción del deber jurídico de impedir la comisión del delito o posición de garante (STS 1480/1999, 13 de octubre)» (SAP MU 1249/2014).

Responsabilidad Administrativa

Cabe añadir como sanción, las medidas de suspensión o revocación de la certificación obtenida como DPD, por parte de la AEDP.

Conviene precisar que como norma general no responderá personalmente por incumplimiento de las obligaciones de la normativa, lo que puede interpretarse que lo que ha querido la normativa al excluirlo de responsabilidad es proteger la institución del DPD, ya que una interpretación contraria, donde el ET o RT le pueda transferir la responsabilidad por los incumplimientos a la normativa en su organización, terminará por desalentar que personas quieran ocupar posiciones de DPD.

Pero lo que no puede negarse es que por la posición y funciones que desempeña se encuentra expuesto personalmente a un riesgo inherente por una mayor exposición al riesgo penal, ya que tiene acceso al conocimiento de hechos o actos delictivos que pueda y deba impedir.

2.4. Régimen sancionador en materia de protección de datos

Con el régimen sancionador previsto en el RGPD la cuestión de la responsabilidad por posibles incumplimientos a las normas sobre tratamiento de datos, tomó especial envergadura y muchísima preocupación entre RT y ET, teniendo en cuenta que el art. 83 del RGDP prevé abultadas sumas en concepto de multas administrativas de hasta 20.000.000 de euros y hasta el 4% del volumen total del negocio anual global el ejercicio financiero anterior de las empresas.

Como ya hemos mencionado, las estadísticas arrojan que el importe de las multas impuestas por la AEDP viene en franco y sostenido aumento.

A las multas puede sumarse la reclamación de daños y perjuicios como consecuencia de los posibles daños que haya sufrido una persona por infracción a la normativa (art. 82 RGPD).

Según parte de la doctrina, la LOPDGDD, en pleno respeto por la RGPD, adapta la normativa a las exigencias constitucionales derivadas del artículo 25 CE que se traducen en una férrea exigencia de respeto a los principios de legalidad, tipicidad, etc., hasta el punto de equiparar en este ámbito el Derecho administrativo sancionador al Derecho penal (MARTÍNEZ 2019).

Sujetos responsables

Se establece como sujetos responsables los RT y los ET, los representantes de los RT o ET no establecidos en el territorio de la UE, las entidades de certificación y las entidades acreditadas de supervisión de los códigos de conducta (art. 70 LOPDGDD).

Tratamiento diferenciado tienen las entidades públicas, establecidas en el art. 77.1 de la LOPDGDD, las que no serán objeto de sanciones económicas, pudiendo establecer contra ellas la sanción de apercibimiento.

Tanto el art. 24.1 del RGPD como el 28.1 LOPDGDD, establecen la responsabilidad del RT y el ET, quienes no solamente deben de cumplir, sino que deben ser capaces de poder demostrar la aplicación y el cumplimiento, y responderán por responsabilidades de naturaleza administrativa o civil, por incumplimientos a la normativa.

También son responsables por el personal a su cargo y parece oportuno recordar la sentencia del TS, que estableció la responsabilidad del Ayuntamiento por la violación de datos cometida por uno de sus empleados: « […] la responsabilidad de la Administración titular y encargada del fichero [Ayuntamiento de San Sebastián] no puede excusarse en su actuación diligente,

separadamente de la actuación de sus empleados o cargos, sino que es la actuación "culpable" de éstos, consecuencia de la violación de las mencionadas obligaciones de protección del carácter reservado de los datos personales la que fundamenta la responsabilidad de la primera en el ámbito sancionador de cuya aplicación se trata; por actos "propios" de sus empleados o cargos, no de terceros [...] » (STS 705/2021).

El TS en sentencia de este año, volvió a expedirse al respecto: «El responsable del fichero o tratamiento adoptará las medidas necesarias para que el personal conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones, así como las consecuencias en que pudiera incurrir en caso de incumplimiento» (…) El actual Reglamento de la UE 2016/679 (LA LEY 6637/2016) de Protección de datos (considerando 74) dispone que «debe quedar establecida la responsabilidad del responsable del tratamiento por cualquier tratamiento de datos personales realizada por él mismo o por su cuenta» y en el 78 en la redacción de los arts. 24 o 28.1 del Reglamento de la Unión» (STS 543/2022).

Tipos de Sanciones

Las infracciones se clasifican en muy graves, graves y leves, siendo constitutivas de infracciones los actos y conductas referidas en los apartados 4, 5 y 6 del art. 83 RGPD y Título IX de la LOPPDGDD. Califican como infracciones graves los casos que conllevan una violación sustancial de la normativa de protección de datos, tales como la vulneración a alguno de los principios y garantías, sin consentimiento o la invalidez del consentimiento, como también por el uso de los datos para finalidades diversas para las que fueron recogidos, entre otros.

La multiplicidad de tipos de sanciones a las que pueden resultar expuestos los RT y ET, exceden el presente trabajo, ya que nos concentraremos en los relacionados con la figura del DPD. No obstante y siguiendo la exposición del «Análisis práctico de sanciones en materia de protección de datos- divididas por conceptos y por sectores-", que sin ánimo de ser exhaustivos, podemos mencionar algunas sanciones que se corresponden con las particularidades de cada sector en el que se desenvuelva la organización o empresa (DAVARA *et al.* (Coords.) 2021).

Se han establecido sanciones relacionadas con áreas específicas y las más frecuentes, como respecto al tratamiento de datos, privacidad, intimidad, la video vigilancia y grabación en el ámbito laboral, sanciones en la Administración Pública, como difusión de imágenes, información, datos personales sin consentimiento o derivadas de la suplantación de identidad

en redes sociales, en el ámbito sanitario donde la protección de datos goza de una mayor protección por la importancia de los datos que se manejan, de seguros y reaseguros, sindicatos y partidos políticos, por uso de GPS como el desvío de la finalidad propia del sistema de video vigilancia o el acceso indiscriminado al sistema informático de datos por parte de todos los agentes de la policía en fuerzas y cuerpos de seguridad del Estado y sanciones a las comunidades de propietarios.

También se han clasificado por conceptos, donde además de las sanciones en relación con el DPD, que analizaremos en el apartado siguiente, encontramos penas específicas relacionadas a las comunicaciones comerciales, sobre medidas de seguridad, relativas al deber de información, por falta o insuficiencia de políticas de privacidad, respecto a los cookies, sobre ejercicio de los derechos de Acceso, Rectificación, Supresión, Portabilidad y Limitación, desde la óptica del derecho a la indemnización por daños sufridos por vulneración de protección de datos, el consentimiento en Marketing, sanciones derivadas del uso de interés legítimo como base legitimadora, sobre protección de datos desde el diseño y por defecto, transferencias internacionales, brechas de seguridad y derecho al olvido.

Sanciones relacionadas con la figura del DPD

Relativo a las sanciones impuestas y relacionadas con el DPD, mencionaremos tres casos:

1. El Procedimiento N° PS/00417/2019, de la AEDP, se inicia en virtud de un reclamo contra la empresa GlovoApp23, S.L. por la falta de designación del DPD. Conforme fundamentación principal en el art. 37.1.b) del RGPD, debió designar obligatoriamente al DPD ya que atendiendo al tratamiento de datos que realiza, su actividad principal implica observación habitual y sistemática de interesados a gran escala. También se estimó que concurrían circunstancias agravantes del art. 83.2. a) y g) del RGPD, esto es el número de afectados era elevado y además se encontraban afectados en el tratamiento datos identificadores personales básicos. Se impuso una multa de 25.000 Euros.

2. El procedimiento N° PS/00001/2020, de la AEDP, en este el reclamo fue contra un organismo de la Administración Pública, el Ayuntamiento de Huercal, Almería, también por falta de designación del DPD, conforme las previsiones de los arts. 37.1 del RGPD y 34. 1 y 3 LOPDGDD, ya que el Ayuntamiento es una autoridad u organismo público, y como tal tiene el deber de designar DPD. Se impuso sanción de apercibimiento y requerimiento de designación de DPD.

Cabe aclarar que la expresión autoridad u organismo público, refiere a la Administración General del Estado, Comunidades Autónomas, Administración Local, Sector público institucional. Y Conforme el GT29, también incluye organizaciones privadas que lleven a cabo el cumplimiento de funciones públicas o autoridad pública (GTA29 2016).

3. El procedimiento N° PS/00251/2020, de la AEDP, contra la empresa CONSEGURIDAD, S.L, que tiene un sistema de Circuito cerrado de Televisión, donde graba imágenes de todas las personas que entran y trabajan en las instalaciones, por falta de designación de DPD, ya que conforme las previsiones del art. 37.1. b) del RGPD, debió designarlo como en el primer caso analizado y también por previsiones del art. 34. 1.ñ) y 3 LOPDGDD ya que por ser empresa de seguridad privada tiene la obligación de designar DPD. En este caso concurren las circunstancias agravantes del art. 83.2. a) y g) del RGPD, esto es el número de afectados era elevado y además se encontraban afectados en el tratamiento datos identificadores personales básicos. Fue sancionado con multa de 50.000 Euros.

Como se observa de los procedimientos analizados, se han impuesto sanciones por falta de designación de DPD, tanto en establecimientos públicos o privados, que conllevan multas elevadas.

De momento no existe ninguna sanción relativa al tratamiento en gran escala de categorías especiales de datos personales (art. 37.1 RGPD), tampoco la relativa a la LOPDGDD en relación a otro sector de la actividad que no sea del ámbito de la seguridad privada, lo que será sólo cuestión de tiempo que las sanciones por falta de designación o mal desempeño del DPD empiecen a multiplicarse (DAVARA *et al.* (Coords) 2021).

Coincidiendo con Romero, destaco su reflexión: «Se acabaron las excusas. La AEDP ha empezado a actuar de manera decidida contra las organizaciones que no tienen DPD a pesar de estar obligadas por ley [….] en el futuro podrían producirse más sanciones relacionadas con los DPD, por motivos distintos. Uno de ellos podría ser la falta de aptitud de las personas seleccionadas para desempeñar el cargo» (ROMERO 2020, p.1).

2.4.1 El alcance de la Responsabilidad Empresarial: Responsabilidad de Medios

Un tema de gran entidad es la determinación sobre el alcance y límite de responsabilidad de las organizaciones y empresas frente a la seguridad de los datos personales.

El Tribunal Supremo, confirmó una sanción de 40.000 Euros a un ET por la falta de adopción de medidas técnicas necesarias para garantizar la seguridad de los datos «La obligación que recae sobre el responsable del fichero y sobre el encargado del tratamiento respecto a la adopción de medidas necesarias para garantizar la seguridad de los datos de carácter personal no es una obligación de resultado sino de medios, sin que sea exigible la infalibilidad de las medidas adoptadas. Solo resulta exigible la adopción e implantación de medidas técnicas y organizativas, que conforme al estado de la tecnología y en relación con la naturaleza del tratamiento realizado y los datos personales en cuestión, permitan razonablemente evitar su alteración, pérdida, tratamiento o acceso no autorizado» (STS 543/2022).

La reciente sentencia ha sentado el precedente, que la obligación del RT y ET es de medios, de comportamiento o debida diligencia, bastando con adoptar las medidas técnicas y organizativas, realizar una actividad diligente en su utilización a los efectos de conseguir el resultado con medios razonablemente idóneos y suficientes.

Por cuanto no se exige que se asegure garantizar la seguridad de los datos personales y que no exista ninguna filtración a la seguridad, como sería si estuviéramos bajo una obligación de resultado y de cumplir con el objetivo propuesto.

Con esta sentencia «El Tribunal Supremo (TS) ha determinado que la obligación de las empresas de garantizar la seguridad de los ficheros que contengan datos personales de sus clientes es de medios, y no de resultado, por lo que bastaría con establecer medidas "técnicamente adecuadas" y utilizarlas de forma razonable» (EXPANSIÓN 2022, p.1).

«En consonancia con la AEPD y la Audiencia Nacional, el Tribunal Supremo confirma que no basta con diseñar los medios técnicos y organizativos necesarios. También es necesaria su correcta implantación y su utilización de forma apropiada, de modo que el responsable del tratamiento también responderá por la falta de la diligencia en su utilización» (BELOKI 2022, p.7).

La misma interpretación se extrae del análisis conjunto y armonizador del art. 32.1 RGPD que establece la obligación del RT y el ET de aplicar las medidas técnicas y organizativas apropiadas para garantizar un nivel adecuado al riesgo, con el art. 83 del RGPD que establece que de aplicar esas medidas técnicas y organizativas apropiadas, serán un factor de graduación de las multas administrativas.

2.4.2. El DPD como posible atenuante a la responsabilidad empresarial

La importancia de la designación del DPD en las organizaciones, aún en los casos en que no sea obligatorio, podrá ser un elemento de graduación para la imposición de multas, en caso de infracción a la normativa (art. 76 LOPDGDD).

El DPD es una garantía de cumplimiento que es altamente valorada por las Autoridades de Control y ante posibles sanciones, será un atenuante para demostrar y defender la responsabilidad de la empresa y obtener reducción de sanciones. También implicará una reducción significativa de inspecciones (GESDATA CONSULTING 2021).

Porque de esta manera, una empresa, frente a una vulneración o filtración a la seguridad de datos personales, podrá demostrar que realizó todas las diligencias necesarias de conformidad con el principio de responsabilidad demostrada, y a criterio del juez, eximirse o atenuar su responsabilidad y por lo tanto, la cuantía de la multa.

Con ello la designación del DPD será siempre recomendable. De la misma manera, la adhesión a códigos de conducta debidamente aprobados o a un mecanismo de certificación aprobado que podrá servir a los efectos de demostrar la debida diligencia (arts. 32.3 y 83.2.j) RGDP).

El primer código de conducta aprobado en el marco del RGPD, por la AEPD fue promovido por Farmaindustria, que aplica la normativa de protección de datos en la investigación clínica y biomédica, y fármaco vigilancia (AEPD 2020). Luego de ello muchas empresas comenzaron a adoptar códigos de conducta, a fin de adaptarse a los nuevos requerimientos, si bien esos códigos no deben quedar plasmados en papel, tienen que adquirir la virtualidad de consolidar el modelo donde la protección de datos esté dentro de sus propósitos fundamentales.

Ambos elementos, sirven para demostrar el cumplimiento de la responsabilidad proactiva y del RGPD.

Todo lo cual nos lleva a la conclusión de la importancia de contar con una verdadera gestión de datos, desde la captación, almacenamiento, tratamiento y uso de datos personales que poseen las organizaciones, que viene enlazado con la designación de una persona capacitada en el ámbito de la empresa para diseñar los medios técnicos y organizativos necesarios, su correcta implantación y utilización, medidas que crearán una presunción de cumplimiento.

Es sabido, que la contratación de un DPD, así como la implementación de todas estas medidas puede significar un costo elevado para la empresa, pero los mismos se tornarán

imprescindibles y convenientes teniendo en cuenta que las multas que se le pueda imponer de no contar con ellos, pueden ser de una envergadura tal que ponga en jaque la continuidad de la propia empresa.

3. Conclusiones

En el trabajo realizado, partimos del análisis del perfil, funciones, responsabilidades del DPD, el cumplimiento del RGPD y del LOPDPGDD en el marco del principio de Responsabilidad Demostrada y hemos podido extraer las siguientes conclusiones:

Primera. DPD como figura crucial del RGPD: Podemos afirmar que el DPD constituye una piedra fundamental en el cumplimiento de los objetivos del RGPD, representando un engranaje necesario para un efectivo ejercicio del principio de responsabilidad proactiva, siendo su designación siempre recomendable, sea por mandato legal o voluntaria, ya que sirve de como garante de la protección de datos y de un enfoque basado en los riesgos.

Segunda. **DPD excluido del régimen sancionador**: Si bien el RGPD excluye expresamente al DPD de toda responsabilidad personal por incumplimiento de las obligaciones impuestas por la normativa y este principio debe primar en pos de garantizar el cargo del DPD, no ha resultado ser del todo absoluto y adquiere relevancia su posible responsabilidad frente a una complicidad omisiva que la Jurisprudencia ha establecido bajo la concurrencia de determinados requisitos.

Si bien su apoyo y asesoramiento no es determinante en la toma de decisiones, si es enorme la injerencia que tiene sobre el RT y ET en la determinación de medios y fines del tratamiento, quienes por lo general actúan en consecuencia del asesoramiento del DPD. Por lo que habrá que estar atentos a los futuros pronunciamientos de los Tribunales, en vistas de los posibles responsabilidades que pudieran serles impuestas en virtud de supuestos grises que se puedan presentar.

Tercera. DPD como atenuante de responsabilidad: El régimen sancionador previsto por la RGPD, al prever altísimas multas, ha tornado de vital importancia, la cuestión relativa a la responsabilidad por parte de organizaciones y empresas por posibles incumplimientos a las normas sobre tratamiento de datos. Relacionadas con el DPD, ya se han impuesto sanciones por su falta de designación obligatoria tanto en el ámbito público como privado. Para que las

organizaciones puedan verse favorecidas con atenuantes de su responsabilidad, será necesario que la política interna de protección de datos, se traduzca principalmente en designación del DPD aun cuando no sea obligatoria, quien es considerado por las autoridades como garantía de cumplimiento, como así también la adhesión a Códigos de Conducta aprobados y a mecanismos de certificación, medidas que permitirán demostrar que han actuado con la debida diligencia, que han adoptado los medios técnicos y organizativos necesarios que permitan acreditar que se encuentra ajustada a la normativa y orientada a conseguir la protección de datos de las personas.

Cuarta. Cultura corporativa: Las organizaciones deberán implementar una cultura de protección de datos, donde contemplen los nuevos derechos de los ciudadanos y la tecnología debe dar un salto exponencial tanto en calidad como en seguridad, y que en vez de enfrentarse a los derechos de las personas, sirvan para reforzarlos. Que este cambio constituya una manifestación de compromiso social y respeto por los derechos y libertades de las personas, donde la puesta en valor de la cultura de protección de datos, se debe comprometer desde un «*Tone from de top»* consistente, y la bajada de línea en todos los niveles de la organización, esté motivada en la protección de los datos personales.

Quinta. **Ventajas reputacionales**: El DPD se convierte en una pieza clave para las organizaciones, a fin de adoptar sus políticas de protección de datos personales y aporta grandes ventajas competitivas a las empresas que lo designan, aun cuando no sea su designación obligatoria, por sobre las que no cuentan con un DPD, en base a los beneficios de contar con un plan de protección de datos personales, asesorados por un especialista en cumplimiento y protección, visto como un valor añadido a la empresa, que redundará en beneficios reputacionales, frente a las que hagan una mala gestión o uso de sus datos personales, que se traducirá en pérdidas de confianza, con el consiguiente daño en términos de competitividad y en su imagen corporativa.

Sexta. Conciencia Social: Finalmente, y no menos importante debe ser la toma de conciencia de las personas, sobre el valor que tienen sus datos personales, el control del acceso sobre su información, que conozcan sus derechos y los hagan valer, tomando una actitud más proactiva con su información, lo que por otro lado transformará en más equitativa la distribución del poder sobre el uso de sus datos, resultando un engranaje justo y adecuado para un mercado

equilibrado entre ambos derechos, al denunciar a las empresas que vulneren sus derechos en protección de datos.

Séptima. Reflexión final: Consideramos que aún falta un largo camino para consolidar el modelo o cambio cultural necesario, donde la protección de datos, en respeto de la libertad y dignidad del ser humano, reconocida en la Declaración Universal de Derechos Humanos, debe ser la referencia primordial y uno de los pilares fundamentales en el desarrollo de las actividades de las entidades y organismos.

Referencias bibliográficas

Bibliografía

BURZACO SAMPER, M. «Protección de datos personales. Esquemas». Dykinson, S.L., Madrid, 2020. p. 71-81.

DAVARA RODRIGUEZ, M.A., «El delegado de Protección de Datos». Consultor de los ayuntamientos y de los Juzgados: Revista técnica especializada en Administración local y Justicia municipal», núm. 24, 2017, p. 3091-3097.

DAVARA FERNANDEZ DE MARCOS, E. y DAVARA FERNANDEZ DE MARCOS, L. (Coords). «Análisis práctico de sanciones en materia de protección de datos –divididas por conceptos y sectores-» Thomson Reuters Aranzadi. Navarra. 2021, p. 663-685.

GONZALEZ CALVO, M., «La nueva figura del Delegado de Protección de Datos», en Actualidad Jurídica Aranzadi, núm. 939, 2018.

SIMÓN CASTELLANO, P. «El desempeño de las funciones del Delegado de Protección de Datos. Gestión de procesos críticos y casos prácticos.» 1° ed. Madrid: Bosch 2018.

SIMÓN CASTELLANO, P. y BACARIA MARTRUS, J. (Coords.). «Las funciones del delegado de protección de datos en los distintos sectores de la actividad». Wolters Kluwer. Madrid. 2020. p. 27-110.

Enlaces Web

AGENCIA ESPAÑOLA PROTECCIÓN DE DATOS. «Esquema de certificación de Delegados de Protección de Datos (Esquema AEDP-DPD)» [en línea]. 2019 [consulta 30 de marzo de 2022] Disponible en: https://www.aepd.es/sites/default/files/2020-07/esquema-aepd-dpd.pdf

AGENCIA ESPAÑOLA PROTECCION DE DATOS. «La AEPD aprueba el primer código de conducta sectorial desde la entrada en vigor del Reglamento de Protección de Datos» [en línea]. 2022 [consulta 6 de abril de 2022] Disponible en: https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/aepd-aprueba-primer-codigo-conducta-sectorial-desde-entrada-vigor-rgpd

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. Listado de Cumplimiento Normativo [en línea] AEDP, 2018, [consulta 28 de Julio de 2022] Disponible en: guia-listado-de-cumplimiento-del-rgpd.pdf (aepd.es)

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. El manual del DPD [en línea] AEDP, 2019 [consulta 28 de julio de 2022]. Disponible en: https://www.aepd.es/sites/default/files/2019-12/El%20Manual%20del%20DPD%20-%20KORFFGEORGES%20-%20ESP.pdf

ASOCIACION FRANCESA DE CORRESPONSALES DE PROTECCION DE DATOS PERSONALES. « Las buenas razones de designar un DPD». Association française des correspondants à la protection des données à caractère personnel «Les bonnes raisons de designer un dpo». [Consulta 12 de mayo de 2022] Disponible en: https://afcdp.net/les-bonnes-raisons-de-designer-un-dpo/

BELOKI, M « El TS ratifica una sanción de 40.000 por una brecha de seguridad en la protección de datos personales» Datcom Norte [en línea] 2022 [consulta 2 de abril de 2022]. Disponible en: https://www.datcon-norte.com/el-ts-ratifica-una-sancion-de-40-000-por-una-brecha-de-seguridad-en-la-proteccion-de-datos-personales/

CARDONA, M. «Novedades del RGPD y la Figura del delegado de Protección de Datos». Protección de datos y cámaras legislativas: [Seminario celebrado en Vitoria-Gasteiz los días 17 y 18 de enero de 2019], 2019, pp. 97-103 [consulta 30 de marzo de 2022]. ISBN 978-84-949559-2-1. Disponible en:

https://www.legebiltzarra.eus/ic2/restAPI/pvgune_descargar/default/db52f700-281b-4b68-9b21-a6687b637fc6

DAVARA FERNÁNDEZ DE MARCOS, I. «¿Existe la privacidad en internet? CE Noticias Financieras. Spanish Ed., Miami. ContentEngine LLC, a Florida limited liability company. 23 Aug 2021 [consulta 4 de julio de 2022] ID del documento de ProQuest: 2564054464. Disponible en: http://www.espaciotv.es:2048/referer/secretcode/wire-feeds/existe-la-privacidad-en-internet/docview/2564054464/se-2?accountid=142712

DE ZARATE, F. «Protección de Datos multa a Google con 10 millones de euros por vulnerar el derecho al olvido» Cinco Días [en línea] 2022 [consulta 19 de mayo de 2022]. Disponible en: https://cincodias.elpais.com/cincodias/2022/05/18/companias/1652864622_556332.html#:~:text=Protecci%C3%B3n%20de%20Datos%20multa%20a,Cinco%20D%C3%ADas

EL MUNDO «Irlanda multa a Instagram con 405 millones por la mala gestión de datos personales de adolescentes» Elmundo.es [en línea] 2022 [consulta 12 de septiembre de 2022]. Disponible en:

https://www.elmundo.es/economia/empresas/2022/09/06/6316fe8ffc6c836f418b457a.html

EUROPEAN COMMISION. COMMISSION STAFF WORKING PAPER, «Impact Assessment Accompanying the document Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data» {COM(2012) 10 final} {COM(2012) 11 final} {SEC(2012) 73 final} [consulta 1 de agosto de 2022]. Disponible en:

https://www.europarl.europa.eu/cmsdata/59702/att_20130508ATT65856-1873079025799224642.pdf

EXPANSION «El Supremo limita la responsabilidad de las empresas si hay brecha de seguridad de datos» [en línea] 2022 [consulta el 2 de abril de 2022]. Disponible en: https://www.expansion.com/juridico/sentencias/2022/02/23/621683f7468aebd1178b456e.html

GAMERO CASADO, E. «El Delegado de Protección de datos en las Administraciones Públicas: ombudsman de los datos» LA ADMINISTRACION AL DIA [en línea] 2019 [consulta 4 de agosto de 2022]. p.1. Disponible en: https://laadministracionaldia.inap.es/noticia.asp?id=1509261

GESDATA CONSULTING «Beneficios de nombrar un Delegado de Protección de Datos» [en línea] 2021 [consulta 21 de abril de 2022]. Disponible en: https://www.gesdataconsulting.es/beneficios-de-nombrar-un-delegado-de-proteccion-de-datos-dpo/

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 1 de abril de 2022]. Disponible en: https://aepd.es/sites/default/files/2019-09/wp243vol01-es.pdf

LOPEZ ESPINAR, A. «Los alarmantes datos sobre hackeos y como preparares para evitar ataques informáticos», EL CRONISTA [en línea] 2022 [consulta 15 de mayo de 2022]. Disponible en: https://www.cronista.com/columnistas/los-alarmantes-datos-sobre-hackeos-y-como-prepararse-para-evitar-ataques-informaticos/

MARTÍNEZ VÁZQUEZ, F. «El reciente marco de la protección de datos personales (RGPD y nueva LOPDP): las obligaciones del responsable y del encargado, el Delegado de Protección de Datos y el régimen sancionador» Revista Rueda, 2019. [Consulta 5 de abril de 2022] ISSN 2530-030X. p. 51-53. Disponible en:

https://repositorio.comillas.edu/xmlui/bitstream/handle/11531/44945/Revista%20RUEDA.pdf?sequence=-1&isAllowed=y

MIGUEL, de J. «Funciones y responsabilidades del delegado de protección de datos». Economist & Jurist (en línea]. 2018, pp. 50-54 [consulta 2 de abril de 2022]. ISSN 2444-3166. Disponible en: https://ecija.com/wp-content/uploads/2018/02/09_en_portada_VI.pdf

MURGA FERNÁNDEZ, J. P. «Protección de datos, responsabilidad activa y técnicas de garantía» ed. Madrid: Editorial Reus, 2018. [Consulta 21 Jul 2022]. p. 174-189. Disponible en: https://bv.unir.net:2769/es/ereader/unir/120927?page=3.

PWC TAX&LEGAL SERVICES NEWSLETTER. «Breves Regulación Digital: Sanciones entorno a la figura del Delegado de Protección de Datos.» 2020 [Consulta 22 de Julio de 2022]. Disponible en: https://periscopiofiscalylegal.pwc.es/wp-content/uploads/2020/06/Breves-Regulaci%C3%B3n-Digital-Sanciones-DPD-Junio-2020.pdf

REAL ACADEMIA ESPAÑOLA. Diccionario panhispánico del español jurídico [en línea]. [consulta 5 de abril de 2022]. Disponible en: https://dpej.rae.es/lema/delegado-de-protecci%C3%B3n-de-datos

RODRÍGUEZ AYUSO, J. F. «Figuras y responsabilidades en el tratamiento de datos personales». ed. Barcelona: J.M. BOSCH EDITOR, 2019. [Consultado en: 21 Jul 2022]. p. 139-163. Disponible en: https://bv.unir.net:2769/es/ereader/unir/127035?page=1.

ROMERO, I. «Organizaciones sin delegado de protección de datos, en punto de mira de la AEDP» Cinco Días, Madrid, 17 Junio 2020. ProQuest, acceso proporcionado por UNIR Universidad Internacional de la Rioja. [consulta 29 de julio de 2022] Disponible en: https://www.proquest.com/docview/2414129733?parentSessionId=1zk9IfeMR0UUFIYP8A8LzOR7aQaIruvPXCtci42Ot8Y%3D&pq-origsite=summon&accountid=142712

SARACIBAR, E. «Una profesión en alza». Red Seguridad: Revista especializada en seguridad informática, protección de datos y comunicaciones [en línea]. 2017, núm. 76, pp. 62 [consulta 30 de marzo de 2022]. ISSN 1695-3991. Disponible en: https://www.redseguridad.com/revistas/red/076/62/index.html

VELAZQUEZ, R. « El delegado de protección de datos en el entorno de la empresa». Red Seguridad: Revista especializada en seguridad informática, protección de datos y comunicaciones [en línea]. 2017, núm. 76, pp. 58-60 [consulta 30 de marzo de 2022]. ISSN 1695-3991. Disponible en: https://www.redseguridad.com/revistas/red/076/58/index.html

Legislación citada

- De la Unión Europea:

CARTA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA. Diario Oficial de la Unión Europea, 18 de diciembre de 2000, núm. 364/1. [consulta 12 de marzo de 2022]. Disponible en: https://www.europarl.europa.eu/charter/pdf/text_es.pdf

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. Diario Oficial de la Unión Europea, 4 de mayo de 2016, núm. 119/1. [consulta 12 de marzo de 2022]. Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807

DIRECTIVA (UE) 2019/1937 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de octubre de 2019 relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión. Diario Oficial de la Unión Europea, 26 de noviembre de 2019. Núm.305/33. [consulta 12 de marzo de 2022]. Disponible en: https://www.boe.es/doue/2019/305/L00017-00056.pdf

-Española:

LEY ORGÁNICA 3/2018, DE 5 DE DICIEMBRE, DE PROTECCIÓN DE DATOS PERSONALES Y GARANTÍA DE LOS DERECHOS DIGITALES. Boletín Oficial del Estado, 6 de diciembre de 2018, núm. 294, Sec. I, p. 119788. [consulta 12 de marzo de 2022]. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673

Jurisprudencia referenciada

-Tribunal Supremo:

Sentencia del Tribunal Supremo, Sala Segunda de lo Penal, de 16 de septiembre de 2010 (Roj: STS 797/2010 – ECLI: ES: TS: 2010:4836).

Sentencia del Tribunal Supremo. Sala de lo Penal, de 23 de mayo de 2016 (Roj: STS 2112/2016 - ECLI: ES: TS: 2016:2112)

Sentencia del Tribunal Supremo. Sala de lo Contencioso de Madrid, de 15 de febrero de 2021 (Roj: STS 705/2021 - ECLI: ES: TS: 2021:705).

Sentencia del Tribunal Supremo, Sala Tercera, de lo Contencioso-administrativo, sección 3°, Sentencia 188/2022 de 15 de febrero de 2022, Recurso N° 7359/2020 (Roj: STS 543/2022, ECLI: ES: TS: 2022:543).

-Audiencia Provincial:

Sentencia de la Audiencia Provincial de Murcia, de 22 de julio de 2014 (Roj: SAP MU 1249/2014 - ECLI: ES: APMU: 2014:1249).

Listado de abreviaturas

AEPD	Agencia Española de Protección de Datos
Art.	Artículo
Arts.	Artículos
CE	Constitución Española
Coords.	Coordinadores
DPD	Delegado Protección de Datos
EIPD	Evaluación de Impacto de Protección de Datos
ET	Encargado de Tratamiento
GT29	Grupo de trabajo del artículo 29 (actual CEPD)
ISO	Organización Internacional de Normalización

LOPDPGDD	Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales
PbD	Principio de privacidad desde el diseño
PDpD	Principio de privacidad por defecto
PDCA	Planificar, Hacer, Verificar y Actuar
RGPD	Reglamento General de Protección de Datos Personales
RT	Responsable de Tratamiento
SEPD	Supervisor Europeo de Protección de Datos
TI	Tecnologías de la Información
TIC	Tecnologías de la Información y la Comunicación
TS	Tribunal Supremo
UE	Unión Europea