Universidad Internacional de La Rioja

Facultad de Derecho

Máster Universitario en Protección de Datos

La responsabilidad del delegado de protección de datos

Trabajo fin de estudio presentado por:	Grace Guerrero Agila
Tipo de trabajo:	Fin de Máster
Director/a:	María Otazu Serrano
Fecha:	21 de julio de 2021

Resumen

Se define el concepto Jurídico de responsabilidad en el ejercicio de la función atribuida como delegado de protección de datos: se identifica los requisitos para ser delegado de protección de datos y las funciones y atribuciones que éste posee en el marco del Reglamento (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 (Reglamento general de protección de datos) en adelante RGPD, y la Ley Orgánica 3/2018 de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, en adelante LOPDGDD; se señala asimismo, los tipos de responsabilidades existentes, por su objeto y por sujeto y se analiza la posibilidad de que un delegado de protección de datos pueda tener algún tipo de responsabilidad o la posibilidad de que llegue a ser responsable solidario por el incumplimiento de la normativa, pese a la determinación realizada en el Reglamento General de Protección de Datos Personales.

Se realiza una revisión del papel de la Agencia Española de Protección de Datos, en adelante AEPD, generando una comparación con la Dirección Nacional de Registro de Datos Públicos, entidad pública que en el Ecuador tiene actualmente entre sus facultades ejecutar los procesos y regular el sistema de registro de datos públicos y su acceso, con el objeto de garantizar la seguridad jurídica, organización, sistematización e interconexión de la información, eficacia y eficiencia de su manejo, publicidad, transparencia y la implementación de nuevas tecnologías; se revisa algunos fallos del Tribunal Constitucional de España, así como en los informes jurídicos del Gabinete Jurídico No. 0070-2018, No. 0149-2019 y No. 0025-2021 de la Agencia Española de Protección de Datos sobre el delegado de protección de datos y su responsabilidad frente a terceros; además se realiza una revisión de la Resolución de Procedimiento Sancionador, No: PS/00070/2019, por el cual la AEPD sanciona al BANCO BILBAO VIZCAYA ARGENTARIA, S.A. (BBVA) por una infracción de los artículos 13 y 14 del RGPD, tipificada en el artículo 83.5.b) y calificada como leve a efectos de prescripción en el artículo 74.a) de la LOPDGDD, con una multa de 2.000.000 euros (dos millones de euros); y, por una infracción del artículo 6 del RGPD, tipificada en el artículo 83.5.a) y calificada como muy grave a efectos de prescripción en el artículo 72.1.b) de la LOPDGDD, con una multa de 3.000.000 euros (tres millones de euros), y el papel que tuvo el Delegado de Protección de Datos; y,

Finalmente, se analizará el papel del delegado de protección de datos en la Ley Orgánica de Protección de Datos del Ecuador, misma que fue publicada el 26 de mayo de 2021 en el Quinto Suplemento del Registro Oficial No. 459.

Palabras clave: Delegado de protección de datos, funciones, responsabilidad, solidario, daños y perjuicios.

Abstract

We are going to define the legal concept of responsibility in the exercise of the function attributed as a data protection officer; the requirements to be a data protection officer and the functions and attributions that he has in the General Data Protection Regulation (GDPR) and the new Organic Law of Protection of Personal Data and guarantee of Digital Rights (LOPDGDD).

Besides, we are going to analyze the possibility that a data protection officer may have some type of responsibility or the possibility that he or she becomes jointly liable for non-compliance with the regulations analyzed, despite the determination made on GDPR.

We will review the role of the AEPD and the DINARDAP (Ecuadorian entity), also we are going to make a comparison between these two entities. We will review some resolutions of the Constitutional Court of Spain and legal reports of the AEPD about the data protection officer.

Finally, we are going to analyze the role of the data protection officer in the new Organic Law of Protection of Personal Data in Ecuador that it was published on May 26, 2021.

Keywords: Data protection officer, functions, responsibility, jointly liable, damages.

Índice de contenidos

1. Introducción 8

1.1. Justificación del tema elegido 10

1.2. Problema y finalidad del trabajo 11

1.3. Objetivos 11

2. Marco teórico y desarrollo 12

2.1. El delegado de proteccion de datos. 12

2.1.1. Quién puede ser delegado de protección de datos. Requisitos: 13

2.1.2. Funciones y atribuciones del delegado de protección de datos 16

2.1.3. Obligatoriedad de contratar a un delegado de protección de datos 20

2.2. El papel de la Agencia Española de Protección de Datos 22

2.2.1. Revisión de Pronunciamientos de la Agencia Española de Protección de Datos sobre el delegado de protección de datos. 23

2.3. El papel de la Dirección Nacional de Registro de Datos Públicos (DINARDAP) en el Ecuador 27

2.4. La nueva Ley Orgánica de Protección de Datos en el Ecuador y su posición frente al delegado de protección de datos. 29

2.4.1. Principios que consagra la Ley Orgánica de Protección de Datos Personales en el Ecuador..... 30

2.4.2. Derechos que consagra la Ley Orgánica de Protección de Datos Personales en el Ecuador 32

2.4.3. Obligaciones que consagra la Ley Orgánica de Protección de Datos Personales en el Ecuador 33

2.4.4. Mecanismos de tutela que consagra la Ley Orgánica de Protección de Datos Personales en el Ecuador 34

2.5. De la responsabilidad 38

2.5.1. Qué entendemos por responsabilidad. Generalidades: 38

2.5.2. Elementos para el establecimiento de responsabilidad 39

2.5.3. Objetivos del establecimiento de responsabilidades 40

2.5.4. Clases de responsabilidades 40

2.5.4.1. Clasificación por los Sujetos: principal y subsidiario; directo y solidario: ... 40

2.5.4.2. Clasificación por su objeto: Administrativas, civiles culposas y penales: ... 41

2.6. Revisión de fallos del Tribunal Constitucional de España 44

3. Conclusiones 47

Listado de abreviaturas 52

Índice de tablas

Tabla 1. “Cuadro comparativo del delegado de protección de datos personales, según lo normado por el Reglamento General de Protección de Datos vs Ley Orgánica de Protección de datos personales ecuatoriana ”.....37

1. Introducción

Se ha orientado el ánimo de estudio del presente máster y de investigación al terreno de la protección de datos puesto que esta materia en el Ecuador, no ha tenido el desarrollo y la evolución que se ha visto reflejada en España como parte del conglomerado de la Unión Europea con la basta normativa que ha ido desarrollando a los largo del tiempo hasta aterrizar con el desarrollo 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 (Reglamento General de Protección de Datos) y por el que se deroga la Directiva 95/46/CE; y, específicamente en España con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, LOPDGDD.

En el Ecuador, el impulso que ha tenido la administración pública para desarrollar plataformas electrónicas que permitan prestar servicios a la colectividad; es decir, cumplir con el servicio público consagrado en la Constitución de la República del Ecuador en su artículo 227, regido por «los principios de eficacia, eficiencia, calidad, jerarquía, desconcentración, descentralización, coordinación, participación, planificación, transparencia y evaluación»[1], se intensificó con la pandemia generada en marzo del año 2020 a consecuencia de la enfermedad mundial provocada por el SARS-coV 2 conocido también como Covid19, debido a que debían continuar brindando el servicio a los ciudadanos con la normalidad que conllevaría la presencialidad en las instituciones públicas, sin embargo no ha existido la concienciación debida respecto al tratamiento que realizan sobre la base de la información personal al que diariamente acceden como administración pública.

Existe un proyecto de Ley Orgánica de Protección de Datos que en septiembre de 2020 fue tratado en primer debate con el cual se ha pretendido dar los primeros pasos en esta materia; sin embargo, ha transcurrido ya un período considerable de tiempo sin tener mayores avances en la Asamblea Nacional para tratar y publicar esta norma que salvaguarde los derechos, promueva la actividad económica, comercial, de innovación tecnológica, social, cultural, entre

[1] Constitución de la República del Ecuador, 2008. Registro Oficial 449, 20 de octubre de 2008, art. 227. Asamblea Nacional, Comisión Legislativa y de Fiscalización, s.f.), pág. 65.

otras y que delimite los parámetros para un tratamiento adecuado en el ámbito público y privado, de manera que se pueda proteger los datos personales de los ciudadanos que por su giro del negocio traten tanto en las administraciones públicas como en el sector privado, de manera que manejen datos personales que puedan verse afectados por falta de normativa clara que señale cómo deben ser llevados a cabo los tratamientos de datos personales, quiénes son responsables del hacerlo, quiénes prestan sus conocimientos y servicios de asesoramiento, como sería los delegados de protección de datos, estableciendo conductas que puedan afectar dichos datos personales y su tratamiento de manera que se impida el mal uso y abuso de estos datos personales y sobre todo establecer lineamientos claros que ayuden a regular y mantener la observancia de la ley en manos de personas capacitadas que puedan asesorar a las máximas autoridades o personeros de los dos ámbitos: público y privado para el cumplimiento de la norma como sería los delegados de protección de datos.

Con el desarrollo del presente trabajo de fin de máster, se pretende profundizar si los delegados de protección de datos, en el marco del Reglamento General de Protección de Datos y en la Ley Orgánica 3/2018, en el ejercicio de sus funciones, que se ahondará en el presente trabajo podrían llegar a ser responsables de los hechos, acciones u omisiones en el ámbito del ejercicio de sus labores y funciones, pese a la determinación realizada en el RGPD, quizá con una responsabilidad solidaria frente al o los responsables directos del tratamiento de datos personales, para lo cual se realizará una búsqueda y análisis doctrinaria y jurisprudencial que pueda proporcionar pautas o directrices respecto a la duda planteada; y, conceptualizar y ampliar la visión que se presenta en el considerando 146 del RGPD, al limitar la responsabilidad y la consecuente indemnización de daños y perjuicios que pueda sufrir una persona a consecuencia de un tratamiento en infracción del Reglamento, al responsable o el encargado del tratamiento de forma directa o con derecho de repetición en contra de los demás responsables del tratamiento y verificar la posibilidad de que la solidaridad en los casos que amerite, llegue al delegado de protección de datos toda vez que de acuerdo al artículo 38.1 del RGPD «el responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos participe de forma adecuada y en tiempo oportuno en todas las

cuestiones relativas a la protección de datos personales»[2] y lo realice con total independencia y sin injerencia de ninguna índole.

En el presente trabajo se ha visto pertinente incluir un análisis de la Ley Orgánica de Protección de datos personales ecuatoriana, la cual ha sido recientemente publicada el 26 de mayo de 2021 en el Quinto Suplemento del Registro Oficial No. 459, fecha que, para la presentación de este Trabajo de Fin de Máster, resulta oportuno.

1.1. Justificación del tema elegido

Partiendo de que el problema a investigar radica en la falta de establecimiento por parte de los legisladores europeos de la responsabilidad que debería tener un delegado de protección de datos en el ejercicio de sus funciones, sea civil, administrativa o penal, dependiendo de las circunstancias en las que se desarrolle la inacción, acción u omisión, es necesario determinar que una persona que tiene a su cargo la posibilidad de estar dentro de una organización de manera amplia, sin intromisiones y que incluso puede ayudar en el establecimiento desde el diseño de tratamiento de datos, y que tiene injerencia en el actuar dentro de una compañía o entidad pública o privada, es necesario que se analice la posibilidad de que aquella persona que funge como delegado de protección de datos tenga a su cargo la responsabilidad de sus actuaciones u omisiones, las cuales deberán ser orientadas a una base administrativa, civil o penal, cuando existe dolo en el actuar.

Ello es importante para que los responsables o encargados del tratamiento se sientan cien por ciento seguros de que la gestión de protección de datos está amparada por una persona que con conocimiento en la materia coadyuvará a la entidad y que no solo formará parte de una plantilla o será colaborador de la misma para el cumplimiento formal de una disposición reglamentaria y legal, pues en la práctica no puede considerarse únicamente que el responsable de un incumplimiento sea el responsable o encargado del tratamiento, si sus actuaciones están siendo amparadas por la asesoría de un tercero capacitado en la materia que actualmente, no goza de ninguna responsabilidad en su actuar; y, por lo tanto, el

[2] REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Art. 38 numeral 1. Pág. 55

legislador al menos debería considerar la opción de una responsabilidad solidaria del delegado de protección de datos y habilitar recursos administrativos y jurisdiccionales para repetir en contra de ellos después del trámite legal correspondiente.

El presente trabajo ayudará a concienciar de esta realidad a fin de que desde la academia se pueda orientar al legislador a la toma de una decisión enmarcada no solo en la protección de datos sino también en la seguridad jurídica que debe ampararse en todo procedimiento administrativo y legal donde primen derechos de los ciudadanos.

1.2. Problema y finalidad del trabajo

¿El delegado de protección de datos es responsable solidario en el ejercicio de sus funciones frente a terceros por ser partícipe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos y actuar de forma independiente?

1.3. Objetivos

a) Definir que es un delegado de protección de datos y las funciones que se le atribuye en la norma para el ejercicio de sus labores.
b) Analizar el Reglamento General de Protección de Datos y la Ley Orgánica de Protección de datos personales y garantía de los derechos digitales y verificar el tipo de responsabilidad que tiene un delegado de protección de datos frente a terceros por sus acciones u omisiones en el marco del cumplimiento de la normativa en protección de datos.
c) Realizar una comparación de esta figura con la Ley Orgánica de Protección de Datos personales publicada en el Ecuador el 26 de mayo de 2021 en el Quinto Suplemento del Registro Oficial No. 459.

2. Marco teórico y desarrollo

2.1. EL DELEGADO DE PROTECCION DE DATOS.

Esta figura del Delegado de Protección de Datos, en adelante DPD, conforme lo expresa el Grupo de Trabajo sobre Protección de Datos del artículo 29, actualmente denominado Comité Europeo de Protección de Datos[3] no es nuevo, aunque la Directiva 95/46/CE3 no exigía a ninguna organización el nombramiento de un DPD, la práctica de tal designación se ha desarrollado, no obstante, en varios Estados miembros a lo largo de los años[4], en el Reglamento General de Protección de Datos, RGDP, por el que se deroga la Directiva 95/46/CE, surge como parte de la nueva visión que se quiere dar a la protección de datos, dejando atrás la mera gestión de datos y saltando a una nueva etapa con el *uso responsable de la información*.

Así un punto en donde se verifica esta transformación que el legislador ha querido plasmar para la Unión Europea, en general, y para España es la figura del delegado de protección de datos, que también es tratado en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, LOPDGDD.

Dicho esto, nos plantearemos una definición de delegado de protección de datos, pues ni el Reglamento de Protección de Datos ni la Ley Orgánica 3/2018, lo define, por lo que, podemos decir que el delegado de protección de datos es la persona natural / física, o jurídica que posee cualidades profesionales, y conocimientos especializados en Derecho y conocimientos prácticos en materia de protección de datos, cuya finalidad es colaborar y asesorar tanto al Responsable del Tratamiento, en adelante RT como al Encargado del Tratamiento, en adelante, ET, en materia de protección de datos vigilando la observancia y cumplimiento interno del propio RGPD y LOPDGDD en el desarrollo de su giro del negocio.

[3] El Comité Europeo de Protección de Datos en la sesión de 25 de mayo de 2018, asumió las directrices sobre el RGPD aprobadas anteriormente por el Grupo de trabajo del artículo 29

[4] Directrices sobre Delegados de Protección de Datos, adoptadas el 13 de diciembre de 2016. Revisadas por última vez y adoptadas el 5 de abril de 2017. 02 de mayo de 2021. 15:00. Disponible en https://www.aepd.es/sites/default/files/2019-09/wp243rev01-es.pdf.

2.1.1. Quién puede ser delegado de protección de datos. Requisitos:

El delegado de protección de datos como mencionamos en el párrafo anterior podrá ser una persona física o jurídica, siempre que cumpla los requisitos que señala el artículo 37 numeral 5 del Reglamento General de Protección de Datos, esto es que pueda demostrar tener cualidades profesionales y, en particular, conocimientos especializados del Derecho y la práctica en materia de protección de datos y su capacidad para desempeñar las funciones que le son atribuidas.

No es necesario que el DPD cuente con una certificación pues no lo exige como requisito obligatorio el Reglamento General de Protección de Datos; sin embargo, la LOPDGDD, en el artículo 35 refiere que el delegado de protección de datos para demostrar su cualificación podrá tener una titulación universitaria que acredite conocimientos especializados en el derecho y práctica en protección de datos. En este sentido, podemos indicar que como requisitos para ser delegado de protección de datos quien quiera serlo deberá demostrar:

a) **Conocimientos especializados**: el considerando 97 del RGPD indica: «El nivel de conocimientos especializados necesario se debe determinar, en particular, en función de las operaciones de tratamiento de datos que se lleven a cabo y de la protección exigida para los datos personales tratados por el responsable o el encargado»; por su parte, el actual Comité Europeo de Protección de Datos, en su documento Directrices sobre los delegados de protección de datos (DPD), 16/ES WP 243 rev.01, al hablar de conocimientos y habilidades del DPD, menciona que «el nivel de conocimientos requerido no está definido estrictamente pero debe ser acorde con la sensibilidad, complejidad y cantidad de los datos que una organización trata[5]», esto quiere decir que la selección de la persona física o jurídica estará supeditada al giro de negocio de la empresa y al tratamiento que sobre éste realice, verificando si se trata gran cantidad de datos, categorías especiales de datos, o si el tratamiento de datos resulta complejo, si existe transferencia internacional o no de datos; por lo que, el DPD para estos casos deberá tener un mayor nivel de conocimiento para ejecutar sus funciones.

[5] Directrices sobre los delegados de protección de datos (DPD), 16/ES, WP 243 rev.01, GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29, Adoptadas el 13 de diciembre de 2016 Revisadas por última vez y adoptadas el 5 de abril de 2017. 02 de mayo de 2021. 15:00. Disponible en https://www.aepd.es/sites/default/files/2019-09/wp243rev01-es.pdf

b) Cualidades profesionales: ni el RGPD ni la LOPDGDD, determina con claridad que profesionales, refiriéndome dentro de una rama específica, podrán ser considerados para desempeñar las funciones de DPD, así el artículo 37 del RGPD, en su numeral 5 reza que en particular, «tendrá en cuenta los conocimientos especializados del Derecho y la práctica en materia de protección de datos», quizá sugiriendo abogados o doctores en jurisprudencia o ingenieros en sistemas que conozcan en la practica el uso de las nuevas tecnologías que han ido surgiendo con el paso del tiempo; y, el propósito de este trabajo tampoco es delimitar o inclinar una postura a que profesionales deben ser considerados como delegados de protección de datos sino más bien seguir con la línea que ha marcado el legislador.

El Comité Europeo de Protección de Datos, menciona en el documento Directrices sobre los delegados de protección de datos (DPD), 16/ES WP 243 rev.01 que, si bien no existe una delimitación taxativa de las cualidades profesionales, existe una enunciación de características que deberán ser tomadas en cuenta a la hora de una designación así tenemos: conocimientos sobre la legislación y prácticas nacionales y europeas en materia de protección de datos, amplia comprensión del RGPD, conocimiento del sector empresarial y de la organización del responsable del tratamiento, conocimiento de las operaciones de tratamiento que se llevan a cabo en la organización, conocimiento de los sistemas de información y de las necesidades de seguridad y protección de datos del responsable del tratamiento y en caso de una autoridad u organismo público, el DPD debe también poseer un conocimiento sólido de las normas y procedimientos administrativos de la organización.

Y considerando que la tecnología es la promotora de este cambio estructural en materia de protección de datos, el delegado de protección de datos deberá tener cierta competencia digital, es decir, una combinación de conocimientos, habilidades y destrezas, para acceder, analizar, evaluar, reflexionar críticamente, crear y actuar frente a situaciones que se generen en su entorno.

En ese sentido se requieren conocimientos «relacionados con el lenguaje específico básico (textual, numérico, icónico, etc.) y de las principales aplicaciones informáticas que le permitan el acceso a las fuentes y el procesamiento de la información, y el conocimiento de los derechos y las libertades que asisten a las personas en el mundo digital. Como también el desarrollo de diversas destrezas relacionadas con el acceso a

la información, el procesamiento y uso para la comunicación, la creación de contenidos, la seguridad».[6]

c) **Capacidad para desempeñar sus funciones**: este requerimiento que realiza el RGPD, está atado como bien indica el Comité Europeo de Protección de Datos a las cualidades personales de quien actúe como DPD: como la integridad y un nivel elevado de ética profesional, yo añadiría la honestidad y diligencia en el actuar diario que debe tener un DPD, otro punto a considerar son los conocimientos que explicamos en el apartado b) de este documento, y el punto final sería el puesto que ocupa el DPD dentro de la organización.

Con relación a este requerimiento el artículo 37 del RGPD, numeral 6 refiere que el Delegado de Protección de Datos, «podrá formar parte de la plantilla del responsable o del encargado del tratamiento o desempeñar sus funciones en el marco de un contrato de servicios»; esto significa que el DPD, podrá ser parte de la nómina y estar bajo una relación de dependencia con el Responsable o Encargado del Tratamiento, lo cual daría una falsa idea de que el DPD está en una posición de subordinación con su empleador y por este hecho supeditado al cumplimiento de las órdenes que éste emita en la ejecución de sus funciones; sin embargo, es el propio Reglamento General de Protección de Datos el que aclara que un DPD participará de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales.

Asimismo detalla que el DPD estará respaldado en el desempeño de las funciones, que trataremos a continuación, por el responsable o el encargado del tratamiento, facilitándole los recursos necesarios para el desempeño de dichas funciones y el acceso a los datos personales y a las operaciones de tratamiento, de igual forma el responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones, para ello se garantiza de manera explícita que No será destituido ni sancionado por su empleador por desempeñar sus

[6]SIERRA BENÍTEZ, E. «El delegado de protección de datos en la industria 4.0: funciones, competencias y las garantías esenciales de su estatuto jurídico». *Revista Internacional y Comparada de RELACIONES LABORALES Y DERECHO DEL EMPLEO.* 2018, Vol. 6. Núm. 1. Pág. 251. [consulta: 03 de mayo de 2021]. ISSN 2282-2313. Disponible en: https://idus.us.es/bitstream/handle/11441/75161/El%20delegado%20de%20protecci%c3%b3n%20de%20datos%20en%20la%20industria.pdf?sequence=1&isAllowed=y

funciones y rendirá cuentas directamente al más alto nivel jerárquico del responsable o encargado del tratamiento.

La otra forma que establece el RGPD para ocupar el cargo dentro de una entidad de gobierno, en cualquier nivel, o dentro de una empresa privada, es por medio de la suscripción de un contrato de servicios, el cual por su naturaleza es netamente civil y no genera relación de dependencia ni cumplimiento ni satisfacción de beneficios laborales para ser considerado trabajador, pues no lo es.

En cualquiera de los dos casos, el responsable o el encargado del tratamiento deberán comunicar a la autoridad de control, en España, Agencia Española de Protección de Datos y en el resto de los países las autoridades autonómicas de protección de datos, la designación que hagan del delegado de protección de datos.

La LOPDGDD, en su artículo 34 numeral 3 señala «Los responsables y encargados del tratamiento comunicarán en el plazo de diez días a la Agencia Española de Protección de Datos o, en su caso, a las autoridades autonómicas de protección de datos, las designaciones, nombramientos y ceses de los delegados de protección de datos tanto en los supuestos en que se encuentren obligadas a su designación como en el caso en que sea voluntaria», más adelante veremos cuando es obligatorio nombrar un Delegado de Protección de Datos para determinar cuándo puede hacerse una designación de manera voluntaria. La autoridad de control estará en la obligación de mantener una lista actualizada de delegados de protección de datos que será accesible por medios electrónicos.

2.1.2. Funciones y atribuciones del delegado de protección de datos

Es importante conocer cuáles son las funciones que debe desempeñar un delegado de protección de datos para sobre la base de ello ahondar en la responsabilidad que acarrea la persona designada para el ejercicio de dicha función, para ello revisaremos el artículo 39 del Reglamento General de Protección de Datos, el cual determina las funciones que deberá cumplir el Delegado de Protección de Datos, así observamos que, el RGPD, establece 5 literales con los que detalla las funciones mínimas que debe realizar un delegado de protección de datos, las cuales las resumo en estas siguientes tres funciones: a) asesoramiento, b) control y supervisión; y, c) nexo comunicacional.

a) **Asesoramiento**: el DPD, debe asesorar e informar tanto al responsable del tratamiento como al encargado del tratamiento, al personal que labora para cada uno de ellos y que tratan datos de carácter personal de las obligaciones que tienen y les son inherentes para cumplir con las disposiciones del RGPD y la LOPDGDD. Asimismo, deben asesorar para el desarrollo de las evaluaciones de impacto sobre protección de datos cuando el riesgo que se pueda producir con un tratamiento sea alto y se pueda afectar derechos y libertades de los interesados para ello se realizará de manera óptima previo al tratamiento de datos personales, aunque esta función considero que la pueden llevar a cabo en tratamientos ya iniciados a fin de ver mejoras a considerar para cumplir las disposiciones del RGPD por medio de una evaluación continua.

b) **Control y supervisión:** una de las funciones más importantes a criterio personal, es la de control y supervisión que ejerce el DPD, pues en sus manos recae la obligatoriedad de verificar que, la persona jurídica que lo ha contratado cuente con las herramientas adecuadas para cumplir con la normativa en protección de datos personales y solventar aquellas falencias para el efectivo cumplimiento de dichas disposiciones, para ello supervisará que se lleven a cabo las políticas introducidas por la organización, en las cuáles, el DPD ha brindado asesoramiento, supervisará que el personal que labora con tratamiento de datos en la organización cumpla las obligaciones y responsabilidades establecidas para cada rol, lo cual también ha de ser observado por el DPD desde el momento de implementación pues ha brindado asesoramiento para dicho efecto; y,

c) **Nexo de comunicación:** el RGPD, expresa que el DPD, debe actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36[7] del Reglamento ibidem, y realizar consultas, en su caso, sobre cualquier otro asunto. Es decir, es un nexo de comunicación entre el responsable del tratamiento o encargado del tratamiento y la autoridad de control, pues es el encargado de consultar a la autoridad de control cuando a su criterio y de las evaluaciones de impacto efectuadas a un tratamiento de

[7]El artículo 36 del RGPD trata sobre la Consulta previa, está consiste en: 1. El responsable consultará a la autoridad de control antes de proceder al tratamiento cuando una evaluación de impacto relativa a la protección de los datos en virtud del artículo 35 muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para para mitigarlo.

datos éste requiera una aplicación más detallada por la complejidad que pueda entrañar.

Ha de entenderse de igual forma, su función de punto de contacto con la autoridad de control, cuándo esta requiera de información del responsable del tratamiento, en pro del cumplimiento de las atribuciones que el Reglamento General de Protección de Datos le atribuya a la autoridad, en especial como indica el Comité Europeo de Protección de Datos «El DPD actúa como punto de contacto para facilitar el acceso de la autoridad de control a los documentos y la información necesarias para la realización de las tareas mencionadas en el artículo 57, así como para el ejercicio de sus poderes de investigación, correctivos, de autorización y consultivos mencionados en el artículo 58[8]».

Es también punto de comunicación entre el ciudadano y el responsable o encargado del tratamiento, en especial cuando de derechos de los interesados se trata; es decir, derecho de Acceso[9], Rectificación[10] y supresión (Derecho al olvido)[11], limitación del tratamiento[12], portabilidad de datos[13], Oposición y decisiones individuales automatizadas[14], pues si bien en el texto se menciona que es obligación del responsable del tratamiento dar atención a los interesados sobre estos derechos ejercidos, no es menos cierto que dichas solicitudes pueden hacerlas llegar a los delegados de protección de datos, quienes remitirán a los responsables del tratamiento para que éstos proporcionen la información y den la atención debida; y, en ese momento se activa la función de control del DPD, a efectos de que la

8 Directrices sobre los delegados de protección de datos (DPD), 16/ES, WP 243 rev.01, GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29, Adoptadas el 13 de diciembre de 2016 Revisadas por última vez y adoptadas el 5 de abril de 2017. 08 de mayo de 2021. 14:50. Disponible en https://www.aepd.es/sites/default/files/2019-09/wp243rev01-es.pdf

9 REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 27 de abril de 2016. Boletín Oficial del Estado, 04 de mayo de 2016, núm. 119. Artículo 15. Disponible en: BOE.es - Buscar.

10 REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 27 de abril de 2016. Boletín Oficial del Estado, 04 de mayo de 2016, núm. 119. Artículo 16. Disponible en: BOE.es - Buscar

11 REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 27 de abril de 2016. Boletín Oficial del Estado, 04 de mayo de 2016, núm. 119. Artículo 17. Disponible en: BOE.es - Buscar

12 REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 27 de abril de 2016. Boletín Oficial del Estado, 04 de mayo de 2016, núm. 119. Artículo 18. Disponible en: BOE.es - Buscar.

13 REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 27 de abril de 2016. Boletín Oficial del Estado, 04 de mayo de 2016, núm. 119. Artículo 19. Disponible en: BOE.es - Buscar.

14 REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 27 de abril de 2016. Boletín Oficial del Estado, 04 de mayo de 2016, núm. 119. Artículo 20. Disponible en: BOE.es - Buscar

contestación sea emitida dentro de los parámetros contemplados en la normativa pertinente de protección de datos; y, la función de supervisión que debe existir en el seguimiento de parte del DPD a cada derecho ejercido por parte de los interesados.

Así también el DPD, es un nexo de comunicación entre los interesados y la autoridad de control, pues los interesados pueden acceder a sus derechos ante el delegado de protección de datos, antes de acudir a la autoridad de control para hacer efectivos dichos derechos, con lo cual será el DPD quien pondrá en conocimiento del interesado la resolución tomada en el plazo máximo de dos meses desde que recibió la comunicación[15].

Finalmente, es un nexo de comunicación entre los trabajadores o colaboradores dentro de la organización y sus empleadores, así lo señala también el Comité Europeo de Protección de Datos cuando menciona que «es importante que el DPD sea considerado como un interlocutor dentro de la organización y que forme parte de los correspondientes grupos de trabajo que se ocupan de las actividades de tratamiento de datos dentro de la organización» y entre los colaboradores y sus empleadores, pues la posición de los segundos frente a los primeros, puede ocasionar timidez al momento de tener que comunicar cualquier eventualidad dentro de la empresa por miedo a ser separados de sus cargos, por lo que, el DPD deberá ser cauto al momento de recabar información guardando siempre la obligación de secreto de confidencialidad[16].

Por lo que, el espíritu del delgado de protección de datos, enmarcado en la legislación de protección de datos es facilitar y coadyuvar la promoción e implementación de una cultura real de protección de datos, incluso pensando en su actuación desde uno de los nuevos elementos que implementó el RGPD como es la protección de los datos desde el diseño y por defecto.

Pero para poder exigir un adecuado desarrollo de funciones, es imperioso dotar de herramientas que le favorezcan en la búsqueda del cumplimiento normativo, así DE MIGUEL

[15] Ley Orgánica 3/2018, de 05 de diciembre de Protección de Datos Personales y garantía de los derechos digitales. Boletín Oficial del Estado Núm. 294, de 6 de diciembre de 2018. Art. 37. Núm. 1, 23 de abril de 2021, Disponible en BOE.es - Buscar

[16] REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 27 de abril de 2016. Boletín Oficial del Estado, 04 de mayo de 2016, núm. 119. Artículo 38 numeral 5. Disponible en: BOE.es - Buscar

(Pág. 4) menciona «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»[17].

En la norma de protección de datos, estas ideas se plasman en el artículo 38 del RGPD, cuando parafraseando menciona que el responsable como el encargado del tratamiento garantizarán que el DPD actúe de forma oportuna y adecuada en los temas atinentes a la protección de datos, se le dotará de recursos necesarios, acceso a la información, a las operaciones del tratamiento, se le dotará de confianza para que rinda cuentas al nivel jerárquico superior de la organización y se garantizará que no reciba instrucciones que tengan injerencia en su accionar, como tampoco podrán ser objeto de sanciones por el cumplimiento de sus funciones, lo cual se podría entender cuando el DPD está sujeto a una relación de dependencia con el responsable del tratamiento.

2.1.3. Obligatoriedad de contratar a un delegado de protección de datos

El Reglamento General de Protección de Datos detalla cuándo es necesario contratar de manera obligatoria una persona que funja como DPD, su artículo 37 refiere tres casos en donde es necesario su contratación esto es cuando:

a) el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial;
b) las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala, o,

[17] DE MIGUEL, J. «Funciones y Responsabilidades del Delegado de Protección de Datos». Economist & Jurist. P. 4. 11 de abril de 2021. Disponible en https://ecija.com/sala-de-prensa/funciones-responsabilidades-del-delegado-proteccion-datos/.

c) las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales con arreglo al artículo 9 y de datos relativos a condenas e infracciones penales a que se refiere el artículo 10.

Por su lado, la LOPDGDD, en su artículo 34 taxativamente señala qué entidades u organizaciones deben designar a un delegado de protección de datos dentro de ellos están: «a) Los colegios profesionales y sus consejos generales. b) 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. c) Las entidades que exploten redes y presten servicios de comunicaciones electrónicas conforme a lo dispuesto en su legislación específica, cuando traten habitual y sistemáticamente datos personales a gran escala. d) Los prestadores de servicios de la sociedad de la información cuando elaboren a gran escala perfiles de los usuarios del servicio. e) Las entidades incluidas en el artículo 1 de la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito. f) Los establecimientos financieros de crédito. g) Las entidades aseguradoras y reaseguradoras. h) Las empresas de servicios de inversión, reguladas por la legislación del Mercado de Valores. i) Los distribuidores y comercializadores de energía eléctrica y los distribuidores y comercializadores de gas natural. j) Las entidades responsables de ficheros comunes para la evaluación de la solvencia patrimonial y crédito o de los ficheros comunes para la gestión y prevención del fraude, incluyendo a los responsables de los ficheros regulados por la legislación de prevención del blanqueo de capitales y de la financiación del terrorismo. k) Las entidades que desarrollen actividades de publicidad y prospección comercial, incluyendo las de investigación comercial y de mercados, cuando lleven a cabo tratamientos basados en las preferencias de los afectados o realicen actividades que impliquen la elaboración de perfiles de los mismos. l) Los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes. m) Las entidades que tengan como uno de sus objetos la emisión de informes comerciales que puedan referirse a personas físicas. n) Los operadores que desarrollen la actividad de juego a través de canales electrónicos, informáticos, telemáticos e interactivos, conforme a la normativa de regulación del juego. ñ) Las empresas de seguridad privada. o) Las federaciones deportivas cuando traten datos de menores de edad», teniendo como características en común, tratar datos e información a gran escala que puede llegar a ser sensible por la complejidad que conllevaría

su tratamiento, el cual, si no se hiciera de manera sistematizada, adecuada y protegiéndola de cualquier tipo de vulneraciones llegue a afectar los derechos de los interesados o ciudadanos.

El Comité Europeo de Protección de Datos, en su Directriz sobre los delegados de protección de datos (DPD), menciona ciertas recomendaciones para determinar si se está frente a tratamientos a gran escala: **a)** uno de los elementos básicos y lógicos, hasta cierto punto, sería el número de interesados que resultarían afectados por dicho tratamiento, el CEPD, indica que este número puede ser una cifra o una proporción de una población específica o determinada; **b)** otra recomendación es observar el volumen y variedad de elementos de datos a tratar; **c)** la duración que tendrá el tratamiento en el tiempo: continuo, en intervalos, periódicos, entre otros; y, **d)** el alcance geográfico del tratamiento, todo ello, debe ser puesto en marcha por medio de sistemas ordenados y metódicos de recogida, procesamiento y publicación de resultados, lo que se traduce en un tratamiento de datos llevados a cabo por la entidad pública o privada.

2.2. EL PAPEL DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

La Agencia Española de Protección de Datos, es una autoridad administrativa, de derecho público, independiente, con personalidad jurídica y plena capacidad pública y privada, que actúa con plena independencia de los poderes públicos en el ejercicio de sus funciones.

Se rige por el Reglamento General de Protección de Datos, la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales, y supletoriamente se regirá por las normas citadas en el artículo 110.1 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

La AEPD, tiene como funciones las establecidas en el artículo 57 del Reglamento General de Protección de Datos, dentro de las cuáles está el velar por la privacidad y la protección de datos de la ciudadanía aplicando las disposiciones normativas que son propias. Y está de dotada de los poderes que se establecen en el artículo 58 del Reglamento ibidem, dentro de los cuales están los poderes de investigación, poderes correctivos, poderes de autorización y consultivos, cada uno de los cuáles con atribuciones que se materializan con actos emitidos por esta a autoridad que deben estar sujetos a las garantías adecuadas, incluida la tutela judicial efectiva y al respeto de las garantías procesales, establecidas en el Derecho de la Unión y de los Estados miembros.

De su página web, se aprecia que el objetivo de dicho espacio es, por un lado, fomentar que las personas conozcan sus derechos y las posibilidades que la Agencia les ofrece para ejercerlos y, por otro, que los sujetos obligados tengan a su disposición un instrumento ágil que les facilite el cumplimiento de la normativa, por lo tanto el papel de la AEPD está orientado a ser la autoridad de control de cumplimiento de las disposiciones del RGPD y ser una entidad no solo coercitiva sino proactiva y preventiva que fomenta el conocimiento de las normas a aplicar y es además fuente de asesoramiento técnico y legal para la ciudadanía y profesionales interesados en la protección de datos personales.

Dentro de uno de sus apartados en la página web, se encuentran los acápites "Informes y Resoluciones", la cual se subdivide en: Normativa, Informes Jurídicos, Resoluciones, Registro de normas corporativas vinculantes, Registros de código de conducta y Circulares, espacio del que revisaremos algunas resoluciones que traten sobre el delegado de Protección de Datos.

2.2.1. Revisión de Pronunciamientos de la Agencia Española de Protección de Datos sobre el delegado de protección de datos.

- La Agencia Española de Protección de Datos, en tratándose del delegado de protección de datos, ha emitido la resolución con la cual se modifica el Esquema de Certificación de delegados de Protección de Datos (Esquema AEPD – DPD). Nacional, a través del cual busca ofrecer seguridad y fiabilidad tanto a los profesionales de la privacidad como a las empresas y entidades que van a incorporar esta figura a sus organizaciones, de manera que tanto el responsable como el encargado de tratamiento seleccionen a profesionales que se han certificado previamente por la Entidad Nacional de Acreditación (ENAC) a fin de que tanto las entidades públicas como privadas que tengan la obligatoriedad como las que voluntariamente deseen unan a sus organizaciones al DPD certificado para el mejor cumplimiento de las obligaciones en la materia de protección de datos.
- De igual forma, el Gabinete Jurídico ha emitido el informe Jurídico No. 0070-2018, en el que se plantea la consulta en referencia a la elaboración de las fichas con los datos tanto de víctimas mortales como de víctimas no mortales en actuaciones de violencia de género y las medidas de seguridad que se debe adoptar, en donde la AEPD se pronuncia con relación al DPD, estableciendo que le corresponde al responsable del tratamiento, con la ayuda, en su caso, del delegado de protección de datos (DPD), la

determinación de las concretas medidas necesarias para la seguridad y confidencialidad de los datos manejados, en este sentido ratifica el papel que tiene el delegado de protección de datos de asesor en materia de protección de datos y la obligatoriedad del responsable del tratamiento de implementar las medidas que considere pertinentes como parte de su responsabilidad conforme lo establece el artículo 24 del RGPD.

- En el Informe Jurídico No. 0149-2019, del Gabinete Jurídico, al analizar el acceso por terceros a información que contiene datos de carácter personal de participantes en procesos públicos de contratación de personal cuando uno de los criterios de valoración es la condición de víctima de violencia de género, refiere al informe 70/2018 en lo atinente a la seguridad del tratamiento de este tipo de datos, indicando nuevamente que corresponde al responsable del tratamiento, con la ayuda, en su caso, del delegado de protección de datos (DPD), la determinación de las concretas medidas necesarias para la seguridad y confidencialidad de los datos manejados aplicando en todo caso el principio de limitación de exactitud y finalidad. De esta manera se mantiene la línea de que el papel del delegado de protección de datos es de asesor o facilitador en materia de protección de datos y la obligatoriedad y responsabilidad recae en el responsable del tratamiento o en el encargado.
- En el Informe Jurídico 0025/2021, del Gabinete Jurídico, al pronunciarse respecto de la solicitud de información efectuada por un parlamentario de la Junta General del Principado de Asturias, calificada y admitida a trámite por la Mesa de la Cámara, sobre la relación de altos cargos y cargos directivos del Principado de Asturias, sus organismos autónomos, entes públicos y empresas públicas a los que se les ha suministrado alguna de las vacunas contra el COVID-19, se ha pronunciado sobre el DPD, su papel fundamental dentro del nuevo modelo de responsabilidad activa que establece el RGPD al indicar que le corresponde en armonía con el responsable del tratamiento ser obligatoriamente designado en los supuestos en que «el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial», y se ha pronunciado sobre ciertas facultades que tiene dentro de las que encontramos:
    a) Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les

incumben en virtud del Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros.

b) Supervisar el cumplimiento de lo dispuesto en el Reglamento General de Protección de Datos, en disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales.
c) Ofrecer asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35 (apartado c).
d) Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36 del RGPD, y realizar consultas, en su caso, sobre cualquier otro asunto.
e) Asesorar al responsable o encargado el tratamiento cuándo éstos tengan dudas respecto de las bases de legitimación de los tratamientos a ser impuestos o implementados en alguna entidad.
f) Elevar a consulta del Gabinete Jurídico, cuando tenga dudas respecto de asuntos legales o jurídicos que no puedan ser absueltos con los pronunciamientos proporcionados por la AEPD.
g) Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36 del RGPD.

El informe cita los artículos 38.1 y 39.2 en los cuales se conmina a garantizar que el DPD, participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales y que desempeñe sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento, sin embargo, no se pronuncia sobre algún tipo de responsabilidad específica para el DPD.

Por otra parte, en la resolución que emite la AEPD, en contra del BANCO BILBAO VIZCAYA ARGENTARIA, S.A. (BBVA) en la Resolución de Procedimiento Sancionador, No: PS/00070/2019, (BBVA) por una infracción de los artículos 13 y 14 del RGPD, tipificada en el artículo 83.5.b) y calificada como leve a efectos de prescripción en el artículo 74.a) de la

LOPDGDD, con una multa de 2.000.000 euros (dos millones de euros); y, por una infracción del artículo 6 del RGPD, tipificada en el artículo 83.5.a) y calificada como muy grave a efectos de prescripción en el artículo 72.1.b) de la LOPDGDD, con una multa de 3.000.000 euros (tres millones de euros), el papel que tuvo el Delegado de Protección de Datos, es de mero conector o cooperador con la entidad reguladora, así lo menciona la resolución al indicar:

> «(…) Correlativamente, el artículo 31 del RGPD establece la obligación de los responsables y encargados del tratamiento de cooperar con la autoridad de control que lo solicite en el desempeño de sus funciones. Para el caso de que éstos hayan designado un delegado de protección de datos, el artículo 39 del RGPD atribuye a éste la función de cooperar con dicha autoridad (…)»[18]

En esta resolución una de las alegaciones de BBVA, es que la AEPD, debió correr traslado al DPD de BBVA a fin de que éste resuelva las reclamaciones en un plazo de un mes, y ponga en conocimiento de la autoridad dichas respuestas; menciona que se lo ha hecho en 4 de las 5 reclamaciones, y que al haber transcurrido un tiempo perentorio de 10 meses sin actuación de la AEPD antes de iniciar el procedimiento aplicaría la caducidad del ejercicio sancionatorio. Por su parte, la AEPD, refuta dicha alegación al indicar que:

> «(…) Del mismo modo, el ordenamiento jurídico interno, en el artículo 65.4 de la LOPDGDD, ha previsto un mecanismo previo a la admisión a trámite de las reclamaciones que se formulen ante la Agencia Española de Protección de Datos, que consiste en dar traslado de las mismas a los delegados de protección de datos designados por los responsables o encargados del tratamiento, a los efectos previstos en el artículo 37 de la citada norma, o a éstos cuando no los hubieren designado, para que procedan al análisis de dichas reclamaciones y a darles respuesta en el plazo de un mes. Se trata de un trámite potestativo, de modo que este traslado se lleva a cabo si la Agencia así lo estima.»[19]

En este sentido, la Agencia establece que no se abrió una fase previa de investigación, por cuanto es una facultad potestativa conforme lo señala el artículo 67 de la LOPDGDD, sin embargo, se corrió traslado al DPD de BBVA, pero que dicho traslado no fue satisfactorio, por

[18] Resolución Agencia Española de Protección de Datos. Procedimiento sancionatorio No. PS/00070/2019 contra Banco Bilbao Vizcaya Argentaria, S.A. (BBVA)
[19] Resolución Agencia Española de Protección de Datos. Procedimiento sancionatorio No. PS/00070/2019 contra Banco Bilbao Vizcaya Argentaria, S.A. (BBVA)

lo que, a los efectos previstos en su artículo 64.2 de la LOPDGDD, se acordó admitir a trámite las reclamaciones presentadas mediante acuerdos que fueron debidamente notificados a los reclamantes.

De la lectura de la resolución, cabe indicar que al delegado de protección de datos, únicamente se le atribuye la facultad de colaborador con la AEPD, para el ejercicio de sus funciones, al respecto no se indica nada de la responsabilidad que podría acarrear para el delegado de protección de datos una posible falta de diligencia y seguimiento a las reclamaciones que se hiciera por parte de 4 personas, a quienes si dio contestación; y más bien, la AEPD dirige su análisis, claro está para proceder a sancionar a la entidad financiera sobre el fondo del asunto en que, BBVA pretende aducir que dicho período de tiempo donde la AEPD no habría realizado alguna actuación avala la política de privacidad de BBVA o que durante ese tiempo cese la responsabilidad de la entidad en el cumplimiento de la norma, pues BBVA conocía las reclamaciones formuladas y conocía también que no existía pronunciamiento alguno de esta Agencia al respecto.

Para mi criterio existe una muestra de falta de diligencia del DPD en el seguimiento de las actuaciones en las que ya ha formado parte por haber sido notificado de las reclamaciones, y que nada hizo al respecto de las mismas, como para verificar si estaban o no en trámite, si estaban asignadas a un responsable o el seguimiento básico como diligencia debida que se da cuando se está a cargo de un trámite administrativo o judicial y no hace nada al respecto lo que termina en una sanción para el responsable del tratamiento; pero bajo la línea indicada de la AEPD nada se dice al respecto.

2.3. EL PAPEL DE LA DIRECCIÓN NACIONAL DE REGISTRO DE DATOS PÚBLICOS (DINARDAP) EN EL ECUADOR

La Dirección Nacional de Registro de Datos Públicos, es una institución del Estado ecuatoriano adscrita al Ministerio de Telecomunicaciones, creada mediante la Ley Orgánica del Sistema Nacional de Registro de Datos Públicos, el 24 de marzo del 2010 y publicada en el Registro Oficial No. 162 del 31 de marzo del 2011, como organismo de derecho público, con personería jurídica, autonomía administrativa, técnica, operativa, financiera y presupuestaria, responsable de dirigir, organizar, regular, gestionar, desarrollar, coordinar, controlar y evaluar el Sistema Nacional de Registro de Datos Públicos, para la obtención, procesamiento y

provisión de datos públicos, directamente y a través de entidades que conforman el Sistema a escala nacional e internacional.

La DINARDAP fue creada para convertirse en una eficiente institución de gestión de datos públicos sobre personas naturales y jurídicas para proveer información válida a usuarios calificados, está dotada de infraestructura física y tecnológica necesaria a nivel nacional; recursos humanos y económicos necesarios y suficientes, con la misión de iniciar y articular el proceso de conexión del Sistema de Registro de Datos Públicos que permitan alcanzar el acceso y la transparencia de la información registral pública, usando las nuevas tecnologías y garantizando la seguridad jurídica en el marco constitucional y legal vigente.

La DINARDAP, ha sido la entidad que ha articulado el uso de las tecnologías de la información y ha definido los programas informáticos y demás aspectos técnicos para cumplimiento obligatorio por parte de las dependencias de Registros Públicos para el sistema interconectado y control cruzado de datos, y para mantenerlo en correcto funcionamiento permitiendo a los ciudadanos acceder a su información por medio del uso del internet pues mantiene una interconexión con la información que reposa en los registros. Ha garantizado el derecho de los titulares de dichos datos que exijan las modificaciones o rectificaciones en dichos registros o bases de datos, siempre que no vulneren disposiciones legales, u órdenes judiciales o administrativas, de igual forma ha garantizado la supresión de información siempre que no afecte o cause perjuicios a derechos de terceras personas, presentando para ello la correspondiente resolución administrativa o sentencia judicial.

Si bien esta entidad desde su creación no ha sido la encargada de regular, controlar o sancionar el incumplimiento de las disposiciones referentes al tratamiento de datos personales y a la libre circulación de estos datos, pues no ha existido en Ecuador una ley de protección de datos, si ha sido la encargada de promover políticas que permitan estandarizar, consolidar y administrar la base única de datos de todos los registros públicos, la que es alimentada por todos los integrantes del Sistema de manera digitalizada de sus archivos, de forma actualizada y simultánea conforme ésta se produzca, promoviendo de igual forma el uso responsable de la información bajo el cumplimiento de estándares técnicos que impidan la caída del sistema, el robo de datos, la modificación o cualquier hecho que pueda afectar la información pública, lo cual se intensificó en el año 2020 con el surgimiento de la pandemia declarada por la OMS, a causa del SARS COV2, lo que agilizó el uso de las tecnologías de la

información para acceder a los servicios que brinda el Estado a los ciudadanos, trasladando la atención presencial a una atención virtual que debía cumplir con los mismos estándares de calidad y seguridad en el uso y manejo de la información.

Actualmente la DINARDAP, con la reciente publicación de la Ley Orgánica de Protección de Datos Personales, tiene la atribución de «controlar y supervisar que las entidades pertenecientes al Sistema Nacional de Registros Públicos incorporen mecanismos de protección de datos personales, así como dar cumplimiento a las disposiciones establecidas en la Ley Orgánica de Protección de Datos Personales, su reglamento de aplicación y demás normativa que la Autoridad de Protección de Datos Personales dicte para el efecto»[20] y «tratar datos procedentes del Sistema Nacional de Registros Públicos o de cualquier otra fuente, para realizar procesos de analítica de datos, con el objeto de prestar servicios al sector público, al sector privado y a personas en general, así como generar productos, reportes, informes o estudios, entre otros. Se utilizarán medidas adecuadas que garanticen el derecho a la protección de datos personales y su uso en todas las etapas del tratamiento como, por ejemplo, técnicas de disociación de datos.»[21]

2.4. LA NUEVA LEY ORGÁNICA DE PROTECCIÓN DE DATOS EN EL ECUADOR Y SU POSICIÓN FRENTE AL DELEGADO DE PROTECCIÓN DE DATOS.

En el Ecuador, desde el año 2019, se empezó a pensar, desarrollar y redactar un proyecto de Ley Orgánica de Protección de Datos, debido a que de acuerdo con una investigación que realizó el equipo de investigación de vpnMentor[22], dirigido por Noam Rotem y Ran Locar, se encontró una gran filtración de datos que abarcaba la violación de datos confidenciales de identificación personal a nivel individual de unos 20 millones de personas ecuatorianas en un servidor ubicado en Miami, propiedad de la compañía ecuatoriana Novaestrat[23], lo cual considero fue el punto de partida para concienciar al legislador sobre el uso de los datos y la

[20] Ley del Sistema Nacional de Registro de Datos Públicos, Asamblea Nacional del Ecuador, Registro Oficial S. No. 162 de 31 de marzo de 2010. Art. 31. Numeral 14.
[21] Ley del Sistema Nacional de Registro de Datos Públicos, Asamblea Nacional del Ecuador, Registro Oficial S. No. 162 de 31 de marzo de 2010. Art. 31. Numeral 15.
22 Fawkes, "Report: Ecuadorian Breach Reveals Sensitive Personal Data, VpnMentor, 2019. Disponible en https://www.vpnmentor.com/blog/report-ecuador-leak/
23 Empresa regulada por la Superintendencia de Compañías Valores y Seguros, constituida en el año 2017, dedicada a la prestación de servicios de consultoría que brinda servicios en análisis de datos, marketing estratégico y desarrollo de software.

información de una manera adecuada por parte de quienes llegan a ser tenedores de los mismos, denominados responsables, encargados o corresponsables de dichos datos.

Así tras dos debates llevados a cabo el 9 y 11 de febrero de 2021, el primero; y, 10 de mayo de 2021, el segundo, la Asamblea Nacional del Ecuador, aprobó el proyecto de Ley Orgánica de Protección de Datos Personales, la cual fue publicada en el registro oficial No. 459 Quinto Suplemento de 26 de mayo de 2021, con lo cual entró en vigencia la Ley con el objetivo de «garantizar el ejercicio del derecho a la protección de datos personales que incluye el acceso y decisión sobre información y datos de este carácter así como su correspondiente protección. Para dicho efecto, regula, prevé y desarrolla principios, derechos obligaciones y mecanismos de tutela.»[24]

La entidad que se encargará del control y la vigilancia de garantizar la protección de los datos personales de los ciudadanos será el Superintendente de Protección de Datos, quien deberá ser Profesional del Derecho, de Sistemas de Información, de Comunicación o Tecnologías, con título de cuarto nivel y con experiencia de 10 años en áreas afines a la materia; será elegido de una terna que enviará el Presidente de la República del Ecuador, y se someterá a un proceso de méritos, a un escrutinio público y a impugnación ciudadana.

En la ley, se establece en su disposición transitoria que, en el plazo de 2 años, contados desde su publicación en el registro Oficial entrará en vigencia las medidas correctivas y el régimen sancionatorio el resto de las disposiciones de la ley entrarán en vigencia desde su publicación en el Registro Oficial.

2.4.1. Principios que consagra la Ley Orgánica de Protección de Datos Personales en el Ecuador

En la Ley Orgánica de Protección de Datos Personales, se establecen los principios de:

a) Juridicidad: El que implica que el tratamiento de datos personales se lo haga en apego y cumplimiento de los principios, derechos y obligaciones establecidos en la Constitución de la República, en los instrumentos internacionales, la ley Orgánica de

24 Ley Orgánica de Protección de Datos Personales, Registro Oficial Quinto Suplemento No. 459 de 26 de mayo de 2021. Disponible en: file:///C:/Users/grace/Downloads/Ley%20Org%C3%A1nica%20de%20Protecci%C3%B3n%20de%20Datos%20Personales.pdf

Protección de datos personales, su reglamento (cuando se lo publique), y la jurisprudencia.

b) Lealtad: Lo que implica que el tratamiento debe ser leal para ello los titulares deberán conocer para que se están usando y cómo se los está tratando.
c) Transparencia: El tratamiento de los datos debe ser comunicado a los interesados de manera sencilla con un lenguaje claro y debe ser de fácil acceso.
d) Finalidad: Las finalidades para el tratamiento de datos personales debe ser explícito y legítimo, y comunicados al titular, no puede usarse los datos para tratamientos distintos a menos que se obtenga alguna de las bases de legitimación expuestos para el nuevo tratamiento.
e) Pertinencia y minimización de datos: Los datos personales deben ser pertinentes y usados en la menor cantidad posible únicamente para la finalidad planteada.
f) Proporcionalidad: El tratamiento debe ser oportuno, relevante y no excesivo con relación a las finalidades para las cuales se los trata.
g) Confidencialidad: El tratamiento de los datos debe tener como base el sigilo y el secreto, y no comunicarse para otro fin que no haya sido mencionado desde el principio.
h) Calidad y exactitud: Los datos personales objeto de tratamiento deben ser claros, exactos, íntegros, precisos, completos, comprobables, de tal forma que no se altere su veracidad, se adoptarán medidas razonables en caso de supresión o rectificación sin dilaciones.
i) Conservación: Los datos personales serán conservados por un plazo no mayor al necesario para cumplir la finalidad propuesta, salvo el caso de archivo en interés público, investigación científica, histórica o estadística.
j) Seguridad de datos personales: Las medidas de seguridad técnicas u organizativas serán implementadas por el responsable o encargado del tratamiento, siendo éstas oportunas y adecuadas atendiendo el estado de la técnica.
k) Responsabilidad proactiva y demostrada: El responsable del tratamiento deberá demostrar el cumplimiento de los derechos, principios y obligaciones establecidas en la ley y demostrar haber implementado mecanismos para la protección de dichos datos.

l) Aplicación favorable al titular: En caso de duda sobre los alcances de la protección de datos personales por parte de las autoridades administrativas o judiciales, se aplicarán e interpretarán en el sentido más favorable al titular de datos.
m) Independencia del control: La autoridad de protección de datos deberá actuar de manera independiente y autónoma e imparcial en sus acciones de investigación, prevención y sanción.

Todos estos, guardan estrecha relación con los planteados en el RGPD; sin perjuicio de que se verifican algunos específicos como el de juridicidad y el de aplicación favorable al titular, que coadyuvan al cumplimento veraz de las disposiciones en materia de protección de datos y a garantizar el derecho a sus titulares.

2.4.2. Derechos que consagra la Ley Orgánica de Protección de Datos Personales en el Ecuador

Los derechos que se consagran en la presente ley son:

a) Derecho de información.
b) Derecho de acceso.
c) Derecho de rectificación y actualización.
d) Derecho de eliminación: (supresión).
e) Derecho de oposición.
f) Derecho a la portabilidad.
g) Derecho a la suspensión del tratamiento.
h) Derecho a no ser objeto de una decisión basada única y parcialmente en valoraciones automatizadas.
i) Derecho de niñas, niños y adolescentes a no ser objeto de una decisión basada única y parcialmente en valoraciones automatizadas.
j) Derecho de consulta: Las personas tienen derecho a consultar pública y gratuitamente el Registro Nacional de Protección de datos personales.[25]
k) Derecho a la educación digital: Tanto los estudiantes como los docentes están garantizados de conocer, acceder, aprender, estudiar, formarse y capacitarse en el uso

[25] Ley Orgánica de Protección de Datos personales, Art. 22. Registro Oficial Quinto Suplemento No. 459 de 26 de mayo de 2021. Disponible en: file:///C:/Users/grace/Downloads/Ley%20Org%C3%A1nica%20de%20Protecci%C3%B3n%20de%20Datos%20Personales.pdf

> adecuado, seguro y responsable de las tecnologías de la información y comunicación con énfasis en la protección de datos personales, intimidad, vida privada, autodeterminación.[26]

Los ejercicios de los derechos son ejercidos por el titular de los datos personales, ante el responsable del tratamiento, autoridad de protección de datos personales o jueces competentes de acuerdo con el procedimiento que se establece en la Ley.

Los adolescentes mayores de 15 años y menores de 18 podrán ejercer personalmente sus derechos; los adolescentes mayores de 12 y menores de 15 años; y las niñas y niños ejercitarán sus derechos por intermedio de sus representantes legales.

2.4.3. Obligaciones que consagra la Ley Orgánica de Protección de Datos Personales en el Ecuador

El tratamiento de los datos personales obliga al responsable o encargado del tratamiento a contar con una base de legitimación por alguna de las 8 causas que se establece en el artículo 7, las cuales tienen similitud con las que plantea el artículo 6 del RGPD, pues habla del consentimiento del titular, que sea realizado por el responsable del tratamiento en cumplimiento de una obligación legal, o por orden judicial, que el tratamiento se sustente en el cumplimiento de una misión realizada en interés público, o en ejercicio de poderes públicos, para ejecución de medidas precontractuales solicitadas por el titular o para el cumplimiento de obligaciones contractuales perseguidas por el responsable o encargado del tratamiento o por un tercero legalmente habilitado, para proteger intereses vitales del interesado, cuando el tratamiento de datos consten en base de datos de acceso público, o para satisfacer intereses legítimos del responsable del tratamiento o tercero habilitado siempre que no prevalezca sobre el interés o derechos fundamentales del titular de los datos.

[26] Ley Orgánica de Protección de Datos personales, Art. 23. Registro Oficial Quinto Suplemento No. 459 de 26 de mayo de 2021. Disponible en: file:///C:/Users/grace/Downloads/Ley%20Org%C3%A1nica%20de%20Protecci%C3%B3n%20de%20Datos%20Personales.pdf

2.4.4. Mecanismos de tutela que consagra la Ley Orgánica de Protección de Datos Personales en el Ecuador

Uno de los mecanismos de tutela que se contempla en la Ley Orgánica de Protección de Datos Personales, tiene relación con la obligación de designación de un delegado de protección de datos, el cual es definido en el artículo 4. Términos y definiciones como: «La persona natural (física) encargada de informar al responsable o al encargado del tratamiento sobre sus obligaciones legales en materia de protección de datos, así como de velar o supervisar el cumplimiento normativo al respecto, y de cooperar con la Autoridad de Protección de Datos Personales, sirviendo como punto de contacto entre esta y la entidad responsable de tratamiento de datos.»

De lo expresado en esta Ley, podemos obtener una primera diferencia con lo expresado en el RGPD, pues para la normativa europea, el delegado de protección de datos puede ser una persona física o jurídica, mientras que la legislación ecuatoriana solo puede serlo una persona física.

Ahora bien, también se establece que existe una obligatoriedad de designación, así lo define el artículo 48, al señalar que se designará un delegado de protección de datos en los siguientes casos:

a) Cuando el tratamiento lo lleve a cabo una de las instituciones que conforman el sector público, según lo que dispone el artículo 225[27] de la Constitución de la República del Ecuador, en adelante CRE.
b) Cuando las actividades del tratamiento requieran un control permanente, sistematizado por su volumen, alcance, naturaleza o finalidad.
c) Cuando se refieran a tratamientos a gran escala de categorías especiales de datos.
d) Cuando el tratamiento no se refiera a datos relacionados con la seguridad nacional o defensa del Estado que adolezcan de reserva ni fuesen secretos.

[27] El artículo 225 de la Constitución de la República del Ecuador, CRE, define que comprende el sector público: 1. Los organismos y dependencias de las funciones Ejecutiva, Legislativa, Judicial, Electoral y de Transparencia y Control Social. 2. Las entidades que integran el régimen autónomo descentralizado. 3. Los organismos y entidades creados por la Constitución o la ley para el ejercicio de la potestad estatal, para la prestación de servicios públicos o para desarrollar actividades económicas asumidas por el Estado. 4. Las personas jurídicas creadas por acto normativo de los gobiernos autónomos descentralizados para la prestación de servicios públicos

Realizando una comparación con la normativa europea, en Ecuador, no se hace una diferenciación al momento de designar un DPD, en el sector judicial, es decir existe la obligación de designarlo de igual forma; y, una situación adicional es que se designará un DPD cuando el tratamiento no se refiera a datos relacionados con la seguridad nacional o defensa del Estado que adolezcan de reserva ni fuesen secretos, mientras que en la normativa europea la tercera consideración es cuando consistan en el tratamiento a gran escala de categorías especiales de datos personales con arreglo al artículo 9 (categorías especiales de datos) y de datos relativos a condenas e infracciones penales a que se refiere el artículo 10, éste último, no se hace mención en la normativa ecuatoriana de manera explícita, aunque a mi criterio puede adecuarse en alguna de las circunstancias indicadas.

El artículo 49 define las funciones que tendrá un delegado de protección de datos, siendo estas agrupadas en 3 funciones: asesorar, supervisar y cooperar.

a) Deberá asesorar al responsable, a su personal, y al encargado del tratamiento sobre las disposiciones de la ley, su reglamento y demás pertinentes en la materia. Deberá asesorar en el análisis de riesgos, en la evaluación de impacto, y evaluación de medidas de seguridad.
b) Deberá supervisar, el análisis de riesgo, la evaluación de impacto y las medidas de seguridad. Deberá supervisar el cumplimiento de las disposiciones que establece la Ley, el reglamento y demás normas que sean aplicables.
c) Deberá cooperar con la autoridad de protección de datos personales, esto es con el Superintendente de Protección de datos. (Figura y entidad que están en proceso de implementación y designación)

Algo novedoso, y lo cual es materia de este Trabajo de Fin de Máster es que, en la legislación ecuatoriana, en la reciente publicación de la Ley Orgánica de protección de Datos Personales, textualmente se indica: «En caso de incumplimiento de sus funciones, el delegado de protección de datos personales responderá administrativa, civil y penalmente, de conformidad con la ley.» estableciendo una responsabilidad administrativa, civil o penal por el incumplimiento de sus funciones dentro de una entidad que requiera de su designación.

Existe aquí una diferenciación muy marcada con la normativa europea en la que, la responsabilidad por las actuaciones en materia de protección de datos la tiene nada más el responsable o encargado del tratamiento, y el DPD, responderá únicamente por la comisión

de un delito, y sólo ahí será sancionado conforme las normas que corresponden al autor del delito tipificado penalmente; sin embargo, el propio RGPD, determina y conmina que la empresa (entendiendo que se trata del responsable o encargado del tratamiento) 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 y el reporte de sus gestiones la hará directamente a los niveles jerárquicos de la misma.

En este sentido, ¿por qué el legislador europeo no ha querido establecer algún tipo de responsabilidad para el DPD si tiene un campo muy amplio de actuación en materia de protección de datos? Le da injerencia para actuar desde el diseño de un tratamiento, le dota de todos los recursos para el ejercicio de sus funciones, tiene garantizado indemnidad, le permite ser punto de contacto entre colaboradores, entre estos y sus empleadores, entre los responsables o encargados del tratamiento y la autoridad de control, pero pese a ello la responsabilidad de los daños y perjuicios causados, cuando incumpla lo dispuesto en dicha norma, recae únicamente en el responsable del tratamiento al igual que en el encargado, quien a su vez responderá cuando incumpla las instrucciones establecidas por el responsable para la prestación del servicio con acceso a datos, quedando exentos de responsabilidad cuando puedan demostrar que no son en modo alguno responsables del hecho que haya causado los daños y perjuicios, provocando que los DPD designados no actúen al cien por ciento, o sean becarios que cumplen una mera formalidad o las personas contratadas no analicen conscientemente las repercusiones de un tratamiento frente a las posibles vulneraciones de derechos de los interesados.

Debería al menos otorgarse la posibilidad de que la responsabilidad sea solidaria con quien define los fines y medios del tratamiento al ser sometidos a una asesoría en dicha materia, pues si bien el Responsable define los medios y los fines de un tratamiento, lo hace bajo un acompañamiento del personal que se supone conoce de la materia, en la práctica el derecho y la tecnología y los riesgos que éstos pueden implicar, ahora, si pese a los consejos del DPD, el Responsable define otros medios y fines y dispone que el encargado lo ejecute contrariando lo sugerido por el DPD, ahí si será una responsabilidad directa del responsable y no se podrá atribuir ningún tipo de responsabilidad al DPD.

A continuación, se establece un cuadro comparativo del delegado de protección de datos personales, según lo normado por el RGPD vs Ley Orgánica de Protección de datos personales ecuatoriana.

REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS- RGPD	**LEY ORGANICA DE PROTECCIÓN DE DATOS PERSONALES, ecuatoriana**
Puede ser persona física o jurídica	Puede ser sólo persona física/natural.
Obligatoriedad de designación: Art. 37 - Cuando el tratamiento lo lleve a cabo una autoridad u organismo público, **excepto** los tribunales que actúen en ejercicio de su función judicial; - las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala, o - Las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales con arreglo al artículo 9 y de datos relativos a condenas e infracciones penales a que se refiere el artículo 10.	Obligatoriedad de designación: Art. 48. - Cuando el tratamiento lo realizan entidades del sector público**, incluido** en el **sector judicial**. - Cuando el tratamiento requiera control permanente, sistematizado por su volumen, alcance, naturaleza o finalidad. - Cuando se refieran a tratamientos a gran escala de categorías especiales de datos - No se refieran a datos de seguridad nacional o defensa del Estado.
Funciones: Art. 39	Funciones: Art. 49

Asesorar, controlar y supervisar y ser punto de contacto entre el RT-ET y la autoridad de control, entre el interesado y el RT-ET, entre colaboradores y empleadores.	Asesorar, controlar, supervisar, cooperar y ser punto de contacto con la autoridad de control y entre el interesado y el RT o ET.
Responsabilidad: No existe una determinación de responsabilidad para el DPD, ésta se orienta únicamente al RT-ET. Si comete delito se sanciona como actor del hecho tipificado.	Responsabilidad: El DPD, tendrá responsabilidad Administrativa, Civil o penal por no cumplimiento de sus funciones.

Fuente: Elaboración propia.

Similitudes:

a) Las dos normativas establecen que la actuación de los delegados de protección de datos debe ser oportuna y apropiada.
b) Desempeña sus funciones sin presiones, obtendrán del responsable y/o encargado del tratamiento los recursos y medios necesarios para el desempeño de funciones.
c) Guardar el secreto de confidencialidad.
d) No podrán ser destituidos o sancionados por el cumplimiento de sus propias funciones.
e) Reportarán directamente al nivel jerárquico superior de la organización.
f) Recibirán capacitación en la materia de protección de datos.
g) Podrán realizar otras actividades, siempre y cuando no exista conflicto de intereses.

2.5. De la responsabilidad

2.5.1. Qué entendemos por responsabilidad. Generalidades:

La responsabilidad es un concepto legal y moral, una obligación inseparable del ejercicio de toda función pública y privada, por la cual, se infringe un deber genérico impuesto a todo ciudadano por el contrato social: no dañar a nadie y en caso de hacerlo, reparar por el daño causado.

La responsabilidad se produce por la acción u omisión en el que incurren los servidores públicos y a mi criterio las personas que trabajan en el sector privado, en el desempeño de un

cargo o puesto de trabajo. La acción es la actividad positiva realizada por el servidor o el trabajador y la omisión consiste en dejar de hacer algo que el servidor público o el trabajador está obligado por la Ley o por sujeción de un contrato.

Para que una responsabilidad se produzca, según la legislación ecuatoriana deberán considerarse varios aspectos como por ejemplo los deberes y obligaciones de los servidores y de terceros, establecidas según la ley o contrato; el poder de decisión o jerarquía del servidor público, el grado de importancia del servicio público que se debe prestar; el grado de culpabilidad tomando en consideración las circunstancias que rodean el acto o hecho; y, finalmente las consecuencias que se derivan de la acción o de la omisión.

Lo cual se puede trasladar al sector privado, para determinar una posible responsabilidad de los trabajadores o colaboradores en el desempeño de sus funciones, como sería el caso de los delegados de protección de datos en empresas privadas obligadas o no a designarlos.

2.5.2. Elementos para el establecimiento de responsabilidad

Para que se produzca responsabilidad, deberá verificarse:

Elementos personales: esto significa que debe existir una persona que causa el daño y una persona que resulta agraviada por dicho daño, siendo la primera la que tiene la obligación de reparar o indemnizar a la segunda por el daño causado;

Un acto u omisión ilícitos: «se trata de una conducta voluntaria por parte del sujeto que transgrede el mandato imperativo consagrado por la Ley: no dañar a nadie. Puede consistir en una conducta positiva, llevar a cabo un comportamiento, o bien omitir una actuación debida.»[28];

Lesión: la que puede ser incumplimiento contractual o de daño, afectando a la persona o al patrimonio del perjudicado, cuando la responsabilidad civil es contractual se pueden establecer penalidades a la hora de indemnizar la lesión y cuando la responsabilidad es extracontractual, será el juez el encargado de valorar la lesión;

[28] GUILLERMO OROZCO PARDO, La Teoría General de la Responsabilidad Civil aplicada al campo de la informática como actividad de riesgo. Disponible en file:///C:/Users/grace/Downloads/Dialnet-LaTeoriaGeneralDeLaResponsabilidadCivilAplicadaAlC-248759.pdf

Nexo causal: entre la lesión y la acción u omisión deberá existir una causalidad que la da origen, tal y como indica la STS de 23/9/91 el resultado ha de ser una consecuencia natural, adecuada y suficiente de la acción, nexo que se rompe cuando concurre el caso fortuito o fuerza mayor;

La culpa: consiste en actos o hechos administrativos que fueron producto de de acciones que denoten impericia, imprudencia, imprevisión, improvisación, impreparación o negligencia, nunca de dolo, pues eso lo convierte en una responsabilidad penal.

2.5.3. Objetivos del establecimiento de responsabilidades

El objetivo del establecimiento de las responsabilidades es la reparación del daño causado en la víctima, la cual no tiene por qué asumir costos por acciones u omisiones contrarias a las disposiciones legales, de manera que se restablezca el orden o el hecho a su estado actual antes del perjuicio causado.

2.5.4. Clases de responsabilidades

Las responsabilidades se clasifican por los sujetos o por el objeto, de la siguiente manera:

2.5.4.1. Clasificación por los Sujetos: principal y subsidiario; directo y solidario:

La Responsabilidad principal es aquella en la que el sujeto está obligado, en primer término, a dar, hacer o no hacer una cosa, por causa de la determinación de la responsabilidad.

La responsabilidad subsidiaria se produce cuando una persona queda obligada en caso de que el responsable principal incumpla lo suyo y su tratamiento se da con menor rigor, pues solo se le exigirá el cumplimiento de la obligación en el caso de que no lo haga el responsable principal, pudiendo posteriormente el segundo solicitar al responsable principal su restitución por medios legales, específicamente por la vía ejecutiva.

La responsabilidad directa se refiere a aquella que recae inmediatamente o en primer término sobre la persona que, por razones de su cargo, incumple determinada actuación u obligaciones.

La responsabilidad solidaria, según el Código Civil ecuatoriano será indivisible; esto es, «in sólidum» sobre dos o más personas. Esta solidaridad se origina cuando son varias las personas que han actuado en determinada toma de decisión que ha producido un perjuicio o irregularidad.

2.5.4.2. Clasificación por su objeto: Administrativas, civiles culposas y penales:

Hay tres clases de responsabilidad por su objeto, siendo estas responsabilidad civil culposa, responsabilidad penal y responsabilidad administrativa.

La responsabilidad civil se deriva del principio general de Derecho de que todo aquel que causa un daño a otro está obligado a repararlo, pagando los daños y perjuicios que se causen a aquella persona. El criterio de responsabilidad civil ha ido evolucionando en el sentido de que no solo una persona que comete un hecho voluntario y consciente (responsabilidad subjetiva) y causa daño a otro debe repararlo, sino que ahora se orienta al resultado y la actividad, (responsabilidad objetiva); es decir ahora, toda actividad susceptible de producir un daño debe contar con la consiguiente obligación de responder si éste se produce.

La responsabilidad civil puede ser contractual o extracontractual; así la primera tiene su origen en el incumplimiento de obligaciones adquiridas entre las partes, para DE ANGEL, «ésta surge cuando se incumple el deber de conducta impuesto por el contrato, pero para valorar ese incumplimiento no sólo cabe atenerse a las cláusulas expresas del convenio, sino a todo aquello que, según su naturaleza, a tenor del artículo 1258 CC sean consecuencias derivadas del mismo merced a la buena fe, el uso y la Ley», citado por Orozco Pardo.

La responsabilidad extracontractual, surge cuando se infringe un deber genérico impuesto a todo ciudadano por el contrato social: no dañar a nadie; de suerte que quien, mediando culpa o negligencia, por acción u omisión, produce un daño a otro, viene obligado a repararlo.

Para OROZCO PARDO, «cada vez se dan más supuestos en los que concurren conductas de varios sujetos, sin que pueda determinarse con claridad siempre quién fue el responsable directo del daño, en razón de ello se ha consagrado un sistema de solidaridad para tales casos pues no cabe hacer una imputación adecuada.»[29], de aquí el concepto de responsabilidad solidaria frente a actuaciones que se realizan y por las cuales no puede pretenderse que la víctima asuma sola los daños que se produzcan, de esta manera el empresario responde por los actos de su trabajador, la Administración por la de sus funcionarios, la sociedad por sus

[29] GUILLERMO OROZCO PARDO, La Teoría General de la Responsabilidad Civil aplicada al campo de la informática como actividad de riesgo. Disponible en file:///C:/Users/grace/Downloads/Dialnet-LaTeoriaGeneralDeLaResponsabilidadCivilAplicadaAlC-248759.pdf

socios, independientemente de que quepa repetir después contra ellos, pues lo prioritario es asegurar la reparación.

En la Constitución de la República del Ecuador, al hablar del sector público, como uno de los ámbitos donde deberá designarse un delegado de protección de datos, se consagra que «Las instituciones del Estado, sus organismos, dependencias, las servidoras o servidores públicos y las personas que actúen en virtud de una potestad estatal ejercerán solamente las competencias y facultades que les sean atribuidas en la Constitución y la ley. Tendrán el deber de coordinar acciones para el cumplimiento de sus fines y hacer efectivo el goce y ejercicio de los derechos reconocidos en la Constitución.»[30]; es decir, es la administración quien determina que las actuaciones de sus funcionarios públicos se harán únicamente si les tienen asignadas facultades y competencias, otorgando taxativamente a sus funcionarios responsabilidad por sus acciones u omisiones, así el artículo 233 reza que: «Ninguna servidora ni servidor público estará exento de responsabilidades por los actos realizados en el ejercicio de sus funciones, o por sus omisiones, y serán responsables administrativa, civil y penalmente por el manejo y administración de fondos, bienes o recursos públicos.», eso no significa que el Estado no pueda accionar contra quienes produjeron el daño pues de igual manera se consagra como uno de los principios para ejercer los derechos que el Estado ejercerá de forma inmediata el derecho de repetición en contra de las personas responsables del daño producido, a través de un proceso contencioso administrativo.

La Ley Orgánica de la Contraloría General del Estado, en el Ecuador, por su parte, trata sobre la responsabilidad civil culposa indicando en el artículo 52 que nace de una acción u omisión, aunque no intencional de un servidor público o de un tercero, autor o beneficiario, de un acto administrativo emitido sin tomar aquellas cautelas, precautelas o precauciones necesarias para evitar resultados perjudiciales, directos o indirectos a los bienes y recursos públicos.

La responsabilidad civil culposa genera una obligación jurídica indemnizatoria del perjuicio económico ocasionado a las instituciones del Estado, calculado a la fecha en que éste se pro

[30] Constitución de la República del Ecuador. Asamblea Constituyente. Registro Oficial 449. De 20 de octubre de 2008. Art. 226

dujo, que nace sin convención, proveniente de un acto o hecho culpable del servidor público o de un tercero, cometido sin intención de dañar.[31]

El que alega deberá probar que los actos o hechos administrativos fueron producto de de acciones que denoten impericia, imprudencia, imprevisión, improvisación, impreparación o negligencia.

En esta línea, si un delegado de protección de datos no cumple con sus funciones y produce un daño sea por una acción o por una omisión, éste deberá responder por el daño causado a través de la predeterminación o glosa de responsabilidad civil culposa o a través de órdenes de reintegro, los cuales los determina únicamente la Contraloría General del Estado, previo la auditoría gubernamental.

La responsabilidad penal es consecuencia de la comisión de delitos tipificados en el Código Penal, y se manifiesta en la aplicación de las sanciones previstas en el mismo Código y en leyes conexas. La responsabilidad penal está supeditada al dolo, es decir a la intención de irrogar daño.

El código penal establecerá conductas típicas que se producirán con ciertos elementos que de comprometerse darán cuenta de la comisión de la conduta tipificada como infracción penal, la cual lleva consigo la imposición de una pena privativa de libertad, afectando así un derecho fundamental del ciudadano, para lo cual, se deberá garantizar el debido proceso hasta la emisión de la resolución con elementos suficientes tendientes a determinar la responsabilidad de tal o cual persona y el cometimiento del delito.

Finalmente, la **responsabilidad administrativa** sobreviene por faltas cometidas en el desempeño del trabajo según las leyes y reglamentos respectivos y su naturaleza es disciplinaria. La responsabilidad administrativa radica en la inobservancia, violación o incumplimiento de las disposiciones legales, atribuciones y deberes que compete a los servidores en razón de sus funciones específicas, sobre la base del interés general pero no procede el establecimiento de la responsabilidad administrativa si no existe norma legal que

[31] Ley Orgánica de la Contraloría General del Estado. Suplemento del Registro Oficial No. 595, 12 de junio de 2002. Reformado por el Segundo Suplemento del Registro Oficial 31, 7 de julio de 2017. Art. 52

la contemple, las sanciones que se aplican por este tipo de responsabilidad son las multa o destitución.

2.6. REVISIÓN DE FALLOS DEL TRIBUNAL CONSTITUCIONAL DE ESPAÑA

- Sentencia 58/2018, de 4 de junio de 2018.

Acción: Recurso de amparo 2096-2016.

Actor: D.F.C. y M.F.C
Demandado: Ediciones El País, SL

Juez: Primera Sala: Don Juan José González Rivas, Presidente, don Andrés Ollero Tassara, don Santiago Martínez-Vares García, don Cándido Conde-Pumpido Tourón, Magistrados, y doña María Luisa Balaguer Callejón (Ponente)

Descripción: Vulneración de los derechos al honor, la intimidad y la protección de datos: derecho al olvido respecto de datos veraces que figuran en una hemeroteca digital; prohibición de indexación de nombres y apellidos como medida limitativa de la libertad de información idónea.

Análisis de la Sala:

Para la Sala, el transcurso del tiempo ha provocado que el interés inicial que el asunto suscitó haya desaparecido por completo, sin embargo, considera que el daño que la difusión actual en la hemeroteca de la noticia produce en los derechos al honor, intimidad y protección de datos personales de las personas recurrentes reviste particular gravedad por el fuerte descrédito en su vida personal y profesional (participación en un delito, drogadicción), por lo que este daño, se estima desproporcionado frente al escaso interés actual que la noticia suscita, y que se limita a su condición de archivo periodístico.

Para la Sala, la alteración de su contenido ya no resulta necesaria para satisfacer los derechos invocados por las personas recurrentes, ya que la difusión de la noticia potencialmente vulneradora de éstos ha quedado reducida cuantitativa y cualitativamente al desvincularla de las menciones de identidad de aquéllas.

Resolución:

«Estimar parcialmente el recurso de amparo: para ello tomó dos decisiones:

1. Declarar que se ha vulnerado el derecho de las personas demandantes de amparo al honor e intimidad (art. 18.1 CE) y a la protección de sus datos personales (art. 18.4 CE).

2. Restablecerlas en su derecho y, declarar la nulidad parcial de la Sentencia del Tribunal Supremo, de 15 de octubre de 2015, únicamente en lo relativo a la revocación del pronunciamiento de la Sentencia de la Sección Decimocuarta de la Audiencia Provincial de Barcelona, de 11 de octubre de 2013, esto es en prohibir la indexación de los datos personales de las demandantes de amparo, en lo que se refiere al nombre y apellidos de las recurrentes, para su uso por el motor de búsqueda interno de la hemeroteca digital gestionada por Ediciones El País, S.L., así como la nulidad de la providencia del mismo Tribunal, de 17 de febrero de 2016, ambas recaídas en el recurso de casación núm. 2772-2013.»

- Sentencia 27/2020, de 24 de febrero de 2020.

Acción: Recurso de amparo 1369-2017.

Actor: La compañía La Opinión de Zamora, S.A.
Demandado: Don I.I.L.

Juez: Segunda Sala: Doña Encarnación Roca Trías, presidenta, y los magistrados don Fernando Valdés Dal-Ré, don Juan Antonio Xiol Ríos, don Pedro José González-Trevijano Sánchez, don Antonio Narváez Rodríguez y don Ricardo Enríquez Sancho

Descripción: Vulneración del derecho a la información (art. 20.1 CE).

Análisis de la Sala:

Para la Sala, no existe proporcionalidad en la noticia publicada en el periódico como ejercicio del derecho a la información, atendiendo a su contenido y finalidad con la colocación de la fotografía que había sido obtenido del Facebook de quien actuó en contra de su hermano y en contra suyo, respecto del respeto a la propia imagen de la persona privada a la que se refiere la noticia publicada en «La Opinión de Zamora», pues los hacia plenamente identificables y por dicho motivo se convertían en noticia pública, sin que fueran personajes públicos.

En consecuencia, la Sala manifiesta que se ha producido un sacrificio desproporcionado en detrimento del derecho a la propia imagen, y la publicación por parte de dicho periódico de la fotografía de la víctima del delito al que la noticia hace referencia, sin su consentimiento, lo

que constituyó una intromisión ilegítima en su derecho a la propia imagen (art. 18.1 CE), el cual, en este caso, no puede encontrar protección en el derecho a comunicar libremente información veraz [art. 20.1 d) CE], constitucionalmente limitado de forma expresa por aquel derecho.

Resolución:

«La Sala resolvió desestimar el presente recurso de amparo.»

De la revisión de estas dos sentencias que he colocado podemos verificar que las Salas realizan un análisis bastante profundo sobre la vulneración de los derechos que los accionantes manifiestan se ha vulnerado en cada caso, lo cual no he entrado a analizar a profundidad pues no es materia de la presente investigación; pero sin embargo, no existe ningún pronunciamiento que se realice sobre el delegado de protección de datos, que en los dos casos debería haberse designado, y la injerencia que éste ha tenido en el marco de las actuaciones de los responsables del tratamiento a quienes han sancionado en las instancias pertinentes previas a llegar al pronunciamiento de este Tribunal Constitucional, con lo cual se mantiene la línea señalada en la norma en materia de protección de datos, que es el no establecimiento de ningún tipo de responsabilidad para esta figura que se ha concretado en el Reglamento General de Protección de Datos y la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales, y que da pie para que se realice un análisis pormenorizado, lo cual se ha pretendido con esta investigación, desde un punto totalmente académico y bajo un criterio netamente personal.

3. Conclusiones

De la investigación realizada, podemos observar que el problema planteado se encuentra latente, y solo se solucionará con la intervención del legislador, la academia podrá impulsar la iniciativa de las reformas que correspondan, el aporte desde esta óptica parte de los objetivos planteados en la investigación, y así podemos concluir que:

PRIMERA: Se ha definido que es un delegado de protección de datos, sus atribuciones y funciones dentro de la legislación europea y ecuatoriana y se ha realizado una comparación entre las dos legislaciones verificando diferencias y similitudes que cada legislación ha adoptado.

SEGUNDA: Del análisis realizado al Reglamento General de Protección de Datos y la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales se ha verificado que al delegado de protección de datos no se le atribuye responsabilidad alguna por el incumplimiento del ejercicio de sus funciones pese a la gran injerencia que tiene en el desarrollo de sus funciones en la empresa a la cual presta el servicio.

TERCERA: Del análisis de la reciente y nueva ley Orgánica de Protección de datos personales ecuatoriana, se aprecia que el legislador ecuatoriano, sí determina tres tipos de responsabilidades para el delegado de protección de datos por el incumplimiento de sus funciones siendo estas, responsabilidad civil, administrativa y la penal.

CUARTA: En la legislación europea No se establece ningún tipo de responsabilidad del delegado de protección de datos, por lo que, debería reformarse este tema y plantearse al menos la posibilidad de que la responsabilidad que se le atribuya al DPD sea solidaria con quien define los fines y medios del tratamiento, pues si bien el responsable del tratamiento define los medios y los fines de un tratamiento lo hace bajo un acompañamiento del personal que se supone conoce de la materia en la práctica en cuanto al derecho, a la tecnología y con conocimiento de los riesgos que éstos pueden implicar, considerando siempre que, si pese a los consejos del delegado de protección de datos el responsable del tratamiento define otros medios y fines y dispone que el encargado del tratamiento lo ejecute contrariando lo sugerido o recomendado por el delegado de protección de datos, el delegado de protección de datos no tenga responsabilidad alguna y sea única y directamente responsabilidad del responsable del tratamiento.

- REFERENCIAS BIBLIOGRÁFICAS

Bibliografía

- BADIOLA, J. y JUÁREZ, A. (2017). Delegado de protección de datos. Camino hacia la certificación y la excelencia. Madrid: Martinco.

- CASTELLANO PERE S. y BACARIA MARTRUS J (Coords.). Las funciones del delegado de protección de datos en los distintos sectores de actividad. Madrid: Wolters Kluwer, 2020.

- DAVARA RODRÍGUEZ, M. Á. Posición y funciones del delegado de protección de datos. Actualidad Administrativa, No. 1. 2018.

- DE MIGUEL, J. Funciones y Responsabilidades del Delegado de Protección de Datos. Economist & Jurist. Disponible en https://ecija.com/sala-de-prensa/funciones-responsabilidades-del-delegado-proteccion-datos/

- DERMISAKY PEREDO, Pablo. La responsabilidad de los funcionarios públicos. Revista Boliviana Der. v. 13 Santa Cruz de la Sierra ene. 2012. ISSN 2070-8157. Disponible en: http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2070-81572012000100002#:~:text=La%20responsabilidad%20es%20un%20concepto,otro%20est%C3%A1%20obligado%20a%20repararlo.

- FERNÁNDEZ SCAGLIUSI, María de los Ángeles. La subjetivización de la responsabilidad administrativa. Universidad de Sevilla. Disponible en: https://idus.us.es/bitstream/handle/11441/96653/La%20subjetivizaci%c3%b3n%20de%20la%20responsabilidad%20administrativa%20.pdf?sequence=1&isAllowed=y

- GONZÁLEZ CALVO, M. La nueva figura del delegado de protección de datos. Actualidad jurídica Aranzadi, No. 939, 2018.

- MARTÍNEZ MORIEL, I. «El delegado de protección de datos como garante de la privacidad en las organizaciones». Andersen. 30 de mayo de 2017. Disponible en: El delegado de protección de datos como garante de la privacidad en las organizaciones - Andersen in Spain

- MESSÍA DE LA CERDA BALLESTEROS, J. A. Consideraciones y perspectivas del Delegado de Protección de Datos. Revista Aranzadi de Derecho y Nuevas Tecnologías, No. 47, 2018.

- SANTAMARIA RAMOS, F. «El principio de responsabilidad proactiva: una oportunidad para un mejor cumplimiento de la normativa en materia de protección de datos de carácter personal en el ámbito latinoamericano.» Revista de la Faculta de Derecho. 2020, No. 85. e-ISSN: 2305-2546. Disponible en: 22974-Texto del artículo-90374-1-10-20201126.pdf

- SIERRA BENÍTEZ, E. El delegado de protección de datos en la industria 4.0: funciones, competencias y las garantías esenciales de su estatuto jurídico. Revista Internacional y Comparada de RELACIONES LABORALES Y DERECHO DEL EMPLEO. 2018, Vol. 6. Núm. 1. ISSN 2282-2313. Disponible en: https://idus.us.es/bitstream/handle/11441/75161/El%20delegado%20de%20protecci%c3%b3n%20de%20datos%20en%20la%20industria.pdf?sequence=1&isAllowed=y

- ROMERO, I. «Organizaciones sin delegado de protección de datos, en punto de mira de la AEPD» Cinco Días. 17 June 2020. Disponible en: Organizaciones sin delegado de protección de datos, en punto de mira de la AEPD - ProQuest (unir.net)

- Guidelines 07/2020 on the concepts of controller and processor in the GDPR. Disponible en: https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf

- Protección De Datos y Administración Local Guías Sectoriales. Agencia Española de Protección de Datos. Disponible en: https://www.aepd.es/sites/default/files/2019-09/guia-proteccion-datos-administracion-local.pdf

- ESQUEMA DE CERTIFICACIÓN DE DELEGADOS DE PROTECCIÓN DE DATOS DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (ESQUEMA AEPD-DPD). Disponible en: https://www.aepd.es/sites/default/files/2020-07/esquema-aepd-dpd.pdf

Legislación citada

- REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 27 de abril de 2016. Boletín Oficial del Estado, 04 de mayo de 2016, núm. 119. Artículo 15. Disponible en: BOE.es - DOUE-L-2016-80807 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que

respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

- Ley Orgánica 3/2018, de 05 de diciembre de Protección de Datos Personales y garantía de los derechos digitales. Boletín Oficial del Estado Núm. 294, de 6 de diciembre de 2018. Disponible en BOE.es - BOE-A-2018-16673 Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

- Ley orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Boletín Oficial del Estado Núm. 298, de 14 de diciembre de 1999. Disponible en BOE.es - BOE-A-1999-23750 Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

- Constitución de la República del Ecuador, Asamblea Constituyente. Registro Oficial 449. De 20 de octubre de 2008.

- Ley Orgánica de Protección de Datos Personales, Registro Oficial Quinto Suplemento No. 459 de 26 de mayo de 2021. Disponible en: file:///C:/Users/grace/Downloads/Ley%20Org%C3%A1nica%20de%20Protecci%C3%B3n%20de%20Datos%20Personales.pdf

- Ley Orgánica de la Contraloría General del Estado. CONGRESO NACIONAL. Registro Oficial S. 595, de 12 jun 2002.

Páginas Web

- Directrices sobre Delegados de Protección de Datos, adoptadas el 13 de diciembre de 2016. Revisadas por última vez y adoptadas el 5 de abril de 2017. Disponible en: https://www.aepd.es/sites/default/files/2019-09/wp243rev01-es.pdf.

- Informe Jurídico No. 0070-2018 de la Agencia de Protección de Datos. Disponible en https://www.aepd.es/es/documento/2018-0070.pdf.

- Dirección Nacional de Registro de Datos Públicos. Disponible en: https://internetsegura.gob.ec/?wpbdp_listing=direccin-nacional-de-registro-de-datos-pblicos.

- Informe Jurídico No. 0149-2019 de la Agencia de Protección de Datos. Disponible en https://www.aepd.es/es/documento/2019-0149.pdf

- Informe Jurídico No. 0025-2021 de la Agencia de Protección de Datos. Disponible en https://www.aepd.es/es/documento/2021-0025.pdf

- Fawkes, "Report: Ecuadorian Breach Reveals Sensitive Personal Data, VpnMentor, 2019. Disponible en https://www.vpnmentor.com/blog/report-ecuador-leak/

- CONSECUENCIAS ADMINISTRATIVAS, DISCIPLINARIAS, CIVILES Y PENALES DE LA DIFUSIÓN DE CONTENIDOS SENSIBLES. Agencia Española de Protección de Datos. Disponible en: https://www.aepd.es/es/documento/consecuencias-administrativas-disciplinarias-civiles-penales.pdf.

Jurisprudencia referenciada

- Sentencia 58/2018, de 4 de junio de 2018 Recurso de amparo 2096-2016: ES:TC:2018:58. Disponible en: Jurisprudencia (tribunalconstitucional.es)
- Sentencia 27/2020, de 24 de febrero de 2020. Recurso de amparo 1369-2017: ES:TC:2020:27. Disponible en: Jurisprudencia (tribunalconstitucional.es)

Listado de abreviaturas

AEPD: Agencia Española de Protección de Datos.

CE: Constitución Española

CEPD: Comité Europeo de Protección de Datos

CRE: Constitución de la República del Ecuador.

CGE: Contraloría General de Estado

DPD: Delegado de Protección de Datos.

DINARDAP: Dirección Nacional de Registro de Datos Públicos

ET: Encargado de Tratamiento.

LOPDGDD: Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales.

RGPD: Reglamento General de Protección de Datos.

RT: Responsable de Tratamiento.