PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR
FACULTAD DE JURISPRUDENCIA

TRABAJO DE INTEGRACIÓN CURRICULAR PREVIO A LA OBTENCIÓN DEL TÍTULO DE ABOGADO

LA FIGURA DEL DELEGADO DE PROTECCIÓN DE DATOS PERSONALES; ANÁLISIS COMPARATIVO ECUADOR-ESPAÑA

RAÚL ALEJANDRO VIZCAÍNO LLÁNEZ

DIRECTOR: RAMIRO ALEJANDRO RODRIGUEZ MEDINA

Quito, 30.05.2023

Dedicatoria

A dios y a la virgen dolorosa,

A mi familia por su constante apoyo,

A mis amigos por sus consejos y aportes

Agradecimientos

Quiero agradecer a mi familia en general, mis padres y mi hermana cuyo papel en esta travesía fue insuperable sin su apoyo y sus constantes ánimos no hubiese podido llegar tan lejos, sin duda agradezco a la vida el poder tener a mi lado su amor, dedicación y enseñanzas.

A mis amigos y compañeros, cada conversación y cada criterio, cada enseñanza y cada consejo me han permitido crecer como persona, su tiempo a mi lado es el tesoro más grande que he podido disfrutar.

A quienes ya no están a mi lado, aunque la vida nos haya separado, sus sonrisas y compañía siempre viven en mis recuerdos, en el lugar donde estén descansando espero firmemente volverlos a encontrar y compartir juntos este preciado logro.

A la Virgen Dolorosa, aún tengo mucho por mejorar, pero en mi corazón deseo hacerte sentir orgullosa oh madre dolorosa.

Resumen: El presente trabajo de titulación examina la figura del Delegado de Protección de Datos (DPD) en el Ecuador de conformidad con lo previsto en la Ley Orgánica de Protección de Datos Personales expedida el 26 de mayo de 2021, una nueva propuesta de trabajo para una mejor protección de los datos personales de los ciudadanos.

Para tales efectos, en el primer capítulo contextualizaremos aspectos generales relativos del tratamiento de datos personales, su protección dentro del marco jurídico nacional y los mecanismos de ejecución aplicados hasta la creación de la norma especializada y, finalmente; en el segundo capítulo realizaremos un análisis comparativo de los conceptos, funciones, atribuciones especiales, obligaciones y características que rodean a esta novedosa figura en el Ecuador, contrastándola con la normativa española a fin de visualizar distintos aspectos del actual marco normativo ecuatoriano que nos permitirán concluir posibles vacíos, observaciones o recomendaciones a ser consideradas para su aplicación.

Palabras Claves: Delegado de Protección de Datos, tratamiento de datos, protección de datos, derecho fundamental

Abastract: The present graduation thesis examines the figure of the Data Protection Officer (DPO) in Ecuador in accordance with the provisions of the Organic Law on Personal Data Protection issued on May 26, 2021, as a new working proposal for the improved protection of citizens' personal data.

For this purpose, in the first chapter, we will provide a general contextualization of aspects related to personal data processing, their protection within the national legal framework, and the implementation mechanisms applied until the creation of the specialized regulation. Finally, in the second chapter, we will conduct a comparative analysis of the concepts, functions, special powers, obligations, and characteristics that surround this innovative figure in Ecuador, contrasting it with Spanish regulations in order to visualize different aspects of the current Ecuadorian legal framework that will allow us to draw possible gaps, observations, or recommendations to be considered for its implementation.

Keywords: Data Protection Officer, Data processing, data protection, fundamental right.

ÍNDICE

INTRODUCCIÓN

Gracias al avance tecnológico y cultural de cada estado, la normativa de nuestra sociedad actual se ha visto inmiscuida en una constante innovación y adaptación sobre las posibles transgresiones que pueden acarrear los actuales y futuros usos de los medios tecnológicos entre la población global, entre ellos, la transgresión del uso de datos personales y por ende de la intimidad de los individuos. Bajo este enfoque, el actual régimen ecuatoriano ha previsto establecer como derecho fundamental en su marco constitucional el Derecho a la Protección de Datos personales de sus ciudadanos, generando a su vez, una normativa enfocada en su cumplimiento.

El presente trabajo se enfoca en la figura del Delegado de Protección de Datos personales, cuya finalidad se orienta en el asesoramiento y supervisión del tratamiento de datos personales dentro del marco de las actividades de muchas instituciones tanto privadas como públicas. Siendo su incorporación en la actual Ley de Protección de Datos Personales una figura novedosa, cuyo papel en la sociedad ecuatoriana nos invita a analizar el nivel de desarrollo y eficacia de la actual normativa en comparación al de España tomando en cuenta el gran desarrollo doctrinario, jurisprudencial y normativo de este último; para este efecto analizaremos distintos aspectos de la legislación española, con la finalidad de determinar posibles falencias apreciables en el actual régimen normativo y presentar posibles propuestas para su fortalecimiento.

CAPÍTULO I: SOBRE LOS DATOS PERSONALES

1.1. Definición de los Datos Personales en el Ecuador

En la actualidad, la era digital ha encontrado valor en el uso y tratamiento de aquellos datos cuya principal característica implica el identificar o hacer identificable a una persona natural o jurídica de manera individual frente a una población. Al comprender la relevancia de mantener vigilancia en cómo son usados los denominados *datos personales*, es así como la legislación ecuatoriana, a lo largo de su historia, ha presentado distintas posturas y concepciones en su intento por abarcar el mayor contenido de los mismos.

Debemos iniciar mencionando que el Ecuador ha pasado por un proceso de desarrollo en cuanto al entendimiento del concepto de *datos personales* y los componentes que lo rodean, de ello podemos mencionar definiciones tales como:

- Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, expresaba en su artículo innumerado lo siguiente: "Datos personales: Son aquellos datos o información de carácter personal o íntimo, que son materia de protección en virtud de esta ley" (LCEFM,2002, art.inn).

Uno de los aspectos más destacables de esta primera percepción normativa la podemos encontrar en su artículo siguiente, del cual, se reconoce su comprensión sobre conceptos relevantes como el "consentimiento y autorización" otorgado por parte de los titulares de los datos para llevar a cabo únicamente los "fines" para los que se ha dispuesto esa información, los cuales fueron desarrollados por la nueva ley especializada en la materia. *(LCEFM,2002, art.inn).*

- Ley Orgánica de Transparencia y Acceso a la Información Pública, aunque no expone una definición concreta del mismo, en su artículo 6, sobre la información confidencial mencionaba:

> Se considera información confidencial aquella información pública personal, que no está sujeta al principio de publicidad y comprende aquella derivada de sus derechos personalísimos y fundamentales, especialmente aquellos señalados en los artículos 23 y 24 de la Constitución Política de la República. (LOTAIP, 2004, art.6)

- Código Orgánico Integral Penal: No posee una definición concreta sobre los datos personales, no obstante, en su artículo 178 se condena la violación en contra de la intimidad y, como veremos más adelante, mantiene una relación secundaria con la protección de datos.

En la actualidad, la principal definición normativa sobre el término *datos personales*, en nuestra legislación, se encuentra plasmada en la Ley Orgánica de Protección de Datos Personales (en adelante LOPDP), esta define a los datos personales como: "Dato que identifica o hace identificable a una persona natural, directa o indirectamente" (LOPD,2021, art 4).

Definición compartida con la Ley Orgánica de Transparencia y Acceso a la Información Pública, cuyo fondo se distancia de aquellos datos considerados públicos. Si bien el concepto contenido por la normativa especializada no profundiza en los aspectos más relevantes del término referenciado, la Ley del Sistema Nacional de Registros Públicos en su artículo 3, párrafo segundo, menciona que dichos datos deberán ser "[…] completos, accesibles, en formatos libres, sin licencia alrededor de los mismos, no discriminatorios, veraces, verificables y pertinentes, en relación al ámbito y fines de su inscripción […]" (LSNRP,2021, art. 3).

No obstante, pese a que la normativa ecuatoriana no detalla puntualmente cuales aspectos destacan sobre aquellos datos de carácter personal, la doctrina, por su parte, busca profundizar en aquellos factores que lo componen. Lorena Naranjo (2018) expone en su obra "El dato personal como presupuesto del derecho a la protección de datos personales y del hábeas data en Ecuador" que, si bien la normativa protege la información de carácter personal, esta habría dejado inobservada la importancia que involucra al "dato" como fuente primordial de la extracción de "información", por tal, define a los datos personales como:

> Información numérica, alfabética, también imágenes, gráfica y fotográfica, acústica (sonidos y voces) o cualquier otro tipo de información con las condiciones de que puedan ser recogidas, registradas, tratadas o transmitidas y que pertenezcan a una persona física identificada o identificable. (Naranjo, 2018, p. 68)

Ahora bien, para comprender por qué se expone la necesidad de diferenciar entre "dato" e "información" debemos remitirnos a la Sentencia No. 001-14-PJO-CC (2014), en el cual, la Corte Constitucional interpreta a estos conceptos como similares, unidos, cuya distinción se acentúa en el proceso comunicativo que puede adquirir el "dato", lo que le da valor y funcionalidad, lo que puede o no generar vulneración, en otras palabras, la información se constituye por medio de la interpretación de los datos, es así como se vuelve necesario su protección y resguardo ante la posibilidad de su mal uso.

Por medio del pensamiento doctrinario, y en aplicación de la normativa, la Corte Constitucional en su Sentencia No. 1868-13-EP/20, por medio de una interpretación pro

hominem, el máximo intérprete constitucional entiende a los datos personales de forma amplia al considerarlos como:

> Toda información que haga referencia de forma directa o indirecta a cualquier aspecto relativo a una persona o sus bienes, en distintas esferas o dimensiones; es susceptible de ser exigida a través de la garantía de hábeas data. Así se advierte que basta con la información –más allá de la forma en que esté contenida- incluya o comunique un aspecto de la persona –objetivo o subjetivo-; o guarde relación con ella, en función de su contenido, finalidad o resultado, para ser considerada como "dato personal*"*. (CCE-EP-1868-13-EP/20, 2020)

En consecuencia, podemos mencionar que los datos personales mantienen un componente sustancial que es la "Información", la decodificación contenida en los datos permite a quien ejecuta el proceso de tratamiento y uso de datos el poder conocer la información contenida en los mismos.

En el caso de los datos de carácter personal, la comprensión del contenido de los mismos, en cualquier formato perceptible, conocido o por desarrollar, permite identificar y hacer identificable a un individuo, siendo posible conocer características particulares como los denominados datos sensibles.

En otras palabras, los datos personales deben ser considerados en un espectro más amplio, pues tanto la información contenida como los medios utilizados en su tratamiento, al igual que los múltiples usos pueden ocasionar una posible vulneración a sus titulares.

1.2. Sobre la Protección de Datos en el Ecuador

En virtud de lo expuesto, el Ecuador acoge la materia de protección de datos personales como uno de los principales proyectos a fortalecer en el estado, cuyo componente nace con la actual Constitución de la República del Ecuador (2008), texto normativo que reconoce en su artículo 66 inciso 19 como derecho fundamental de los ciudadanos la protección de datos de carácter personal:

> El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley. (CRE,2008, art. 66)

En función de la norma constitucional, se emite la Ley Orgánica de Protección de Datos Personales, publicada en el Registro Oficial 5to Suplemento No. 459 el 26 de mayo de 2021, con la cual busca garantizar el ejercicio del derecho de los denominados Datos

Personales. Siendo uno de los principales objetivos de esta normativa el constituir un mecanismo de garantía en favor del cumplimiento pleno de los derechos fundamentales a la intimidad y privacidad de los ciudadanos, derechos que han sido muchas veces menoscabados por una creciente red de información comercializada que por falta de control y seguridad eficientes han permitido la difusión de información personal con o sin el consentimiento de sus titulares.

Aunque en la actualidad podamos contar con una legislación especializada debemos comprender distintos aspectos que han llevado a la creación de dicha normativa en el Ecuador.

Anteriormente, el ordenamiento jurídico nacional no desarrollaba un criterio propio sobre lo que hoy denominamos "protección de datos personales", como lo explica Luis Ordóñez Pineda:

> En el año 1998 la protección de datos de carácter personal no se hallaba reconocida como un derecho fundamental, y, más bien, sus facultades se ejercían a través de otros derechos civiles como la intimidad personal y familiar, entre otros; y al hábeas data como garantía constitucional. (Ordóñez, 2017, p. 85)

En ese contexto, normativas como el Código Orgánico Integral Penal (COIP) complementaban los vacíos legislativos de esta materia, puesto que, como lo mencionamos anteriormente, tipifica los delitos en contra de los Derechos a la Intimidad tanto personal como del núcleo familiar, esto le ha llevado a convertirse, en el pasado, en una norma suplementaria, incluso de definiciones tales como la ya mencionada Ley de comercio electrónico, firmas electrónicas y mensajes de datos expedida en el año 2002, sobre los datos personales. Y es que, si bien la normativa ecuatoriana tomaba en cuenta a los datos personales como un bien jurídico a ser protegido, previo a la expedición de la normativa especializada, no existían parámetros o delimitaciones establecidas para su adecuado salvaguardo, y como veremos más adelante, su accionar consistía únicamente en la aplicación del *Hábeas Data*.

Es así como se configura el derecho de protección de datos de carácter personal como un mecanismo de protección de la denominada *autodeterminación informativa.* Esta concepción es, para autores como Lorena Naranjo:

> La libertad de un titular respecto de cómo disponer de sus datos personales, cualquiera sea la naturaleza de estos, es decir, no solo aquellos referidos al ámbito de su intimidad o privacidad, sino incluso los aparentemente inocuos (…) y replicar las consecuencias

> indeseadas de valoraciones no deseadas, no autorizadas, equivocadas o inexactas. (Naranjo,2017, p.66).

Por tales efectos la misma autora aclara que la protección de este derecho permite garantizar el cumplimiento de otros derechos inherentes a las personas al considerar la relevancia de la información que se está debatiendo.

En esa misma línea de pensamiento, autores como Felipe Roldan Carrillo consideran que la ya citada autodeterminación informativa se relaciona con dos componentes claves para su protección: el consentimiento y la finalidad.

> El consentimiento es la facultad del titular para decidir acerca de sus datos. Mientras que la finalidad del tratamiento de datos exige un propósito determinado, explícito y legítimo. Así, la clara determinación y correcta regulación de ambos principios es esencial para tener un modelo normativo que haga efectivo el ejercicio de este derecho. (Carrillo, 2021, p. 184)

La protección de datos personales se construye como un mecanismo que garantiza que los titulares puedan decidir libre y voluntariamente sobre el uso de sus datos personales para que puedan mantener un equilibrio entre su vida privada, su intimidad, de aquellos datos que están al conocimiento público, por tal razón, elementos como el consentimiento libre, voluntario e informado, así como la legitimidad propia de la recolección de datos, los fines para los cuales se implementa el tratamiento de datos, se convierten en elementos esenciales a tomar en cuenta ante el creciente desarrollo tecnológico que amenaza cada vez más a la privacidad de los ciudadanos.

1.3. El Hábeas Data y su relevancia en la Protección de Datos Personales

Cuando la normativa ecuatoriana aún se encontraba en desarrollo sobre el contenido en materia de protección de datos, el ejercicio del Derecho al resguardo y cuidado de aquellos datos de carácter personal se los ejecutaba únicamente por medio de la garantía constitucional del *Hábeas Data*. Esta figura tiene sus primeras apariciones en las reformas a la Constitución de 1978, expedida en el año de 1996, sin embargo, su desarrollo sería mayormente visible en normas constitucionales posteriores. En la actualidad, la constitución del 2008 contempla en su artículo 92 el estado de garantía constitucional a la *Acción de Hábeas Data* de la siguiente manera:

> Toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes,

> consten en entidades públicas o privadas, en soporte material o electrónico. Asimismo, tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos.
>
> Las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la ley.
>
> La persona titular de los datos podrá solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación. En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias. Si no se atendiera su solicitud, ésta podrá acudir a la jueza o juez. La persona afectada podrá demandar por los perjuicios ocasionados. (CRE, 2008, art.92)

Acorde a la interpretación de la Corte Constitucional en su sentencia No. 182-15-SEP-CC, de fecha 03 de junio de 2015, el máximo órgano de interpretación constitucional define a este mecanismo de la siguiente manera:

> Es la garantía constitucional que le permite a la persona natural o jurídica, acceder a la información que sobre sí misma reposa en un registro o banco de datos de carácter público o privado a fin de conocer el contenido de la misma y de ser el caso, exigir su actualización, rectificación, eliminación o anulación cuando aquella información le causa algún tipo de perjuicio a efectos de salvaguardar su derecho a la intimidad personal y familiar. (CCE, Nro. 182-15-SEP- CC, 2015)

En relación a lo expuesto, entendemos que la protección de datos de carácter personal implica un aspecto más íntimo de los individuos, aquellos que tienen la capacidad de vulnerar una representación íntima y personal de sus titulares, por tal, la finalidad, en materia de protección de datos, de esta garantía es la de salvaguardar y diferenciar aquella información que no es de carácter público, permitiendo ejecutar a los individuos acciones tales como: actualización, rectificación, eliminación o anulación de información.

Si bien es cierto que este mecanismo ha sido fuertemente utilizado en el ejercicio pleno de los derechos de los ciudadanos, la doctrina considera que su utilidad es válida hasta el desarrollo completo de un marco normativo en la materia, puesto que la práctica del mismo presenta múltiples dificultades.

Es así como debemos cuestionarnos sobre la viabilidad práctica de esta figura en materia de protección de datos. La Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional nos habla del *Habeas Data* en su capítulo IV, en el mismo se nos menciona que será posible interponer dicha acción bajo tres circunstancias: 1) cuando se niegue el acceso a la documentación; 2) exista impedimento entorno a las actuaciones de los

titulares sobre sus datos personales, y; 3) Cuando el uso de la información personal viole un derecho constitucional, salvo mandato del juez.

Autores como María Alejandra Vera y María Belén Vivero (2019) critican la falta de una especificación sobre el tiempo oportuno para la aplicación de esta garantía constitucional, considerando que, ante la negativa de otorgamiento de documentación u aplicación de acciones, no existe un plazo determinado cuando se manifiesta de forma expresa, y se podría generar una ambigüedad en caso de ser tácita, por cuanto sería imposible determinar el momento en que se configura.

En concordancia, la ya mencionada Sentencia 182-15-SEP-CC, del 26 de octubre de 2015, explica que se deberá seguir un "plazo razonable" que deberá ser estudiada por el juez a cargo desde la calificación de la demanda, sin embargo, al no existir una determinación específica sobre dicho "plazo razonable" se podría generar una indefensión y posible afectación al titular de los datos.

Adicionalmente, las autoras explican que de acuerdo al artículo 51 de la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional, sobre la legitimación activa, al otorgar la facultad para presentar esta acción a las personas jurídicas se estaría generando una desnaturalización de esta figura, puesto que son aquellas entidades jurídicas las principales fuentes de afectación en contra de los titulares de los datos. Atendiendo a estas consideraciones, si bien la figura del habeas data comprende un alcance importante en el desarrollo y aplicación de la protección de datos en el país, podemos darnos cuenta que el inevitable desarrollo de la tecnología ha sugerido la necesidad de ampliar la comprensión de conceptos tales como los datos personales.

Aunque la acción de habeas data comprende, en primera instancia, una aplicación correctiva en favor de la protección de datos personales, esta no se configura como una herramienta especializada y por ende actúa en campo general, ante lo cual, la normativa ecuatoriana se vio en la necesidad de desarrollar distintos parámetros y concepciones que se adapten a los tiempos modernos.

1.4. Sobre el tratamiento de datos personales y como opera en el Ecuador

Una vez cubierto los aspectos más destacables de los datos personales y la importancia de su protección y resguardo, debemos comprender en que consiste su "tratamiento" y el cómo nuestra normativa lo percibe. En la actualidad, por medio de la LOPDP (2021), nuestra legislación define al tratamiento de datos como:

> Cualquier operación o conjunto de operaciones realizadas sobre datos personales, ya sea por procedimientos técnicos de carácter automatizado, parcialmente automatizado o no automatizado, tales como: la recogida, recopilación, obtención, registro, organización, estructuración, conservación, custodia, adaptación, modificación, eliminación, indexación, extracción, consulta, elaboración, utilización, posesión, aprovechamiento, distribución, cesión, comunicación o transferencia, o cualquier otra forma de habilitación de acceso, cotejo, interconexión, limitación, supresión, destrucción y, en general, cualquier uso de datos personales. (LOPDP, 2021, art.4)

La Corte Constitucional, por su parte, en su Sentencia No. 2064-14-EP/21, de 15 de marzo de 2021, a través de una interpretación pro homine toma en consideración la definición emitida por la Unión Europea y decide entender al proceso de tratamientos de datos en su sentido más amplio al definirlo como: "[…] cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales". (CCE, Nro. 2064-14-EP/21, 2021)

Como ya hemos mencionado anteriormente, la importancia del dato radica principalmente en su función comunicativa, datos que si bien carecen de relevancia a primera vista carecen de significado e importancia, con su descifrado y comprensión pueden generar una posible vulneración y afectación a sus titulares en caso de no aplicarse para los fines pertinentes, es así como el tratamiento de datos personales permite a quien ejecuta el proceso de tratamiento, el poder mantener un conocimiento y vigilancia de la vida cotidiana; del perfil más íntimo de sus usuarios. En ese contexto, la LOPDP en su artículo 7 establece que el tratamiento de datos tendrá el carácter de legítimo y lícito cuando se cumpla alguna de las condiciones descritas a continuación:

> 1) Por consentimiento del titular para el tratamiento de sus datos personales, para una o varias finalidades especificas;
>
> 2) Que sea realizado por el responsable del tratamiento en cumplimiento de una obligación legal;
>
> 3) Que sea realizado por el responsable del tratamiento, por orden judicial, debiendo observarse los principios de la presente Ley;
>
> 4) Que el tratamiento de datos personales se sustente en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, derivados de una competencia atribuida por una norma con rango de ley, sujeto al cumplimiento de los estándares internacionales de derechos humanos aplicables a la materia, al cumplimiento de los principios de esta Ley y a los criterios de legalidad, proporcionalidad y necesidad;

> 5) Para la ejecución de medidas precontractuales a petición del titular o para el cumplimiento de obligaciones contractuales perseguidas por el responsable del tratamiento de datos personales, encargado del tratamiento de datos personales o por un tercero legalmente habilitado;
>
> 6) Para proteger intereses vitales del interesado o de otra persona natural, como su vida, salud o integridad;
>
> 7) Para tratamiento de datos personales que consten en bases de datos de acceso público; u,
>
> 8) Para satisfacer un interés legítimo del responsable de tratamiento o de tercero, siempre que no prevalezca el interés o derechos fundamentales de los titulares al amparo de lo dispuesto en esta norma. (LOPDP, 2021, art. 7)

Ante lo referido debemos destacar que el tratamiento de datos sigue principalmente el carácter de lícito y consensuado, sin embargo, tal como lo expone la Corte Constitucional en su dictamen Nro.13-18-TI/19, de 13 de mayo de 2019, el tratamiento de datos que carezca de la autorización del titular deberá tener "un fin determinado, explícito, legítimo y autorizado por la ley. El derecho a la protección de datos personales excluye la recopilación arbitraria y caprichosa de estos datos" (CCE, Nro. 2064-14-EP/21, 2019).

CAPÍTULO II: SOBRE EL DELEGADO DE PROTECCIÓN DE DATOS PERSONALES; COMPARATIVA ECUADOR-ESPAÑA

2.1. Concepto del Delegado de Protección de Datos Personales

Como hemos podido visualizar en el contenido del presente trabajo, la importancia de la protección de datos personales en la normativa existente constituye un carácter fundamental en la seguridad de los ciudadanos. Ante el interés de mantener y generar una correcta aplicación de la norma, tanto la legislación ecuatoriana como la española han visto pertinente contemplar a la figura del Delegado de Protección de Datos, en adelante DPD, como integrante del sistema de protección de datos y, como veremos a lo largo del presente capítulo, se constituye en una pieza clave para su adecuado cumplimiento y desarrollo.

Es así como la LOPDP en Ecuador define a la figura del DPD en su artículo 4, Términos y definiciones, como:

> Persona natural 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 del tratamiento de datos. (LOPDP, 2021, art.4).

Debido a que el DPD se establece como una figura novedosa en el marco normativo ecuatoriano, es necesario que contrastemos la percepción actual contenida en la Ley de Protección de Datos Personales con una legislación más desarrollada en el tema como lo es la normativa española.

A diferencia de nuestro marco legislativo, la normativa española no ofrece una definición propia sobre la figura del DPD, no obstante, desde el punto de vista doctrinario se pone a consideración el concepto del mismo tomando en cuenta los factores que lo componen, es así como, según Francisco Durán:

> Únicamente podemos encontrar una definición del delegado de protección de datos si nos remitimos al documento que elaboró la Comisión Europea relativo a la evaluación de impacto sobre la propuesta de Reglamento, donde manifiesta que se trata de: ´Una persona responsable en el seno de un responsable del tratamiento o un encargado del tratamiento de supervisar y monitorear de manera independiente la aplicación interna y el respeto de las norma sobre protección de datos. El DPO puede ser tanto un empleado interno como un consultor externo. (Durán, 2018, p. 134)

Siendo instituida por medio de los articulados 37, 38 y 39 del Reglamento General de Protección de datos (RGPD) en lo que se refiere a la generalidad del concepto del DPD. Para Santamaría Francisco , en referencia a la Directiva 95/46/CE, considera que:

> Este título hace referencia a aquella persona que se encuentra en posesión de una función o mandato (…) participa en el ejercicio de la autoridad cumpliendo el rol de lo que se suele denominar «directivo» en el ámbito de las organizaciones privadas; mientras que, en el de las organizaciones públicas, cumple el papel de aquellos individuos con potestades directivas y de organización de corte fundamentalmente político. (Santamaría, 2020, pp. 151)

Textos emitidos por la Autoridad de Protección de Datos, en respuesta a las múltiples preguntas sobre la correcta aplicación de las disposiciones normativas a ser aplicadas en materia de protección de datos han definido al DPD como:

> Persona física o jurídica, empleado en plantilla o mediante contrato de servicio, que informa y asesora al Responsable, al Encargado y a otros empleados sobre las obligaciones del RGPD y supervisa su cumplimiento, cooperando y actuando como punto de contacto con las Autoridades de Control. (AEPD, 2018, p. 2)

Podemos notar que el punto de vista español toma en consideración a las personas jurídicas como capaces de ejecutar las funciones de un DPD, por un lado esta

determinación permitiría a las instituciones, como pueden ser los centros de asesoría, el poder ampliar sus actividades comerciales, sin embargo, cabe preguntarnos si existe o no una desnaturalización de la figura por cuanto son principalmente las personas jurídicas quienes vulneran los derechos respecto de la protección de datos personales de sus titulares. Como menciona Andrés Salcedo:

> Su actuación vendrá guiada siempre, teniendo en cuenta, la naturaleza, alcance, licitud, contexto y fines del tratamiento, siendo por lo demás, partícipe, de todas las cuestiones de entidad, relativas a protección de datos personales, que ideen o lleven a cabo los respectivos responsables o encargados del tratamiento, debiendo rechazar cualquier manifestación de acoso o de abuso de autoridad, proporcionando siempre toda la información necesaria para el adecuado seguimiento de la actividad, sin ocultar errores o incumplimientos, y procurando subsanar las carencias que se detecten. (Salcedo, 2018, p. 29)

Por tales razones, autores como Suzana Lozano consideran que:

> Para las organizaciones, contar con esta figura, constituirá una garantía, que establece que las empresas deben adoptar las medidas que aseguren razonablemente que están en condiciones de cumplir con los principios, derechos y garantías. (Lozano, 2018, p.25)

2.2. Funciones, Derechos Y Obligaciones del Delegado de Protección de Datos

2.2.1. Funciones y obligaciones

Ante la aplicación de la actual normativa en materia de Protección de datos personales, es relevante para el presente trabajo el exponer las distintas funciones y obligaciones aplicables en el cargo del Delegado de Protección de Datos Personales a contrastar con la normativa española.

Como fue mencionado anteriormente, el Delegado de Protección de Datos Personales (DPD) mantiene una función de control y supervisión en el ejercicio de sus actividades. La actual LOPD, en su articulado 49 establece como sus funciones las siguientes:

> 1) Asesorar al responsable, al personal del responsable y al encargado del tratamiento de datos personales, sobre las disposiciones contenidas en esta Ley, el reglamento, las directrices, lineamientos y demás regulaciones emitidas por la Autoridad de Protección de Datos Personales;
>
> 2) Supervisar el cumplimiento de las disposiciones contenidas en esta Ley, el reglamento, las directrices, lineamientos y demás regulaciones emitidas por la Autoridad de Protección de Datos Personales;

> 3) Asesorar en el análisis de riesgo, evaluación de impacto y evaluación de medidas de seguridad, y supervisar su aplicación;
>
> 4) Cooperar con la Autoridad de Protección de Datos Personales y actuar como punto de contacto con dicha entidad, con relación a las cuestiones referentes al tratamiento de datos personales; y,
>
> 5) Las demás que llegase a establecer la Autoridad de Protección de Datos Personales con ocasión de las categorías especiales de datos personales. (LOPD, 2021, art.49)

Como se visualiza en el presente articulado, el Delegado cumple una función de asesor y supervisor respecto del cumplimiento total de las distintos parámetros y regulaciones emitidos por la Autoridad de Protección de Datos, dicha cualidad denota una fuerte conexión con las autoridades pertinentes, lo cual expone ante el titular un grado de confianza y seriedad a la hora de gestionar el tratamiento de datos.

Es importante destacar que si bien una de las características más prominentes de esta figura implica su relación directa con las autoridades encargadas tanto del tratamiento de datos personales (RT y ET) como de aquellas competentes para su regulación, hasta la presente fecha, la falta de nombramiento de esta última obstruye la naturaleza propia del DPD, puesto que, al no existir una autoridad ante el cual responder por la vigilancia ejercida, se pone en duda la relevancia de la misma, lo cual, puede ocasionar posibles vulneraciones en contra de los titulares de datos personales.

Adicionalmente, es menester recalcar que, conforme se menciona en su apartado final, un DPD puede ejercer otras funciones dispuestas por Autoridad de Protección de Datos Personales, las cuales, si bien no hacen explícitas posibles limitaciones o excepciones, podrían ser aplicadas en el fortalecimiento interno institucional como lo son el apoyo directo en el ejercicio de funciones del encargado o responsable de la protección de datos, siempre que no exista conflicto con la normativa legal vigente contemplada tanto por esta ley como por la Autoridad competente en materia.

En relación al conocimiento propio de las leyes y de las distintas pautas ejercidas en la materia, la LOPD no menciona requisito alguno para la contratación del DPD, por tanto, se expresa la incógnita ¿es necesario que el profesional posea un título de profesional en Derecho para ejecutar dichas funciones? Como veremos más adelante, se entiende que el profesional deberá tener los suficientes conocimientos sobre la ley propia de la materia, además de comprender el funcionamiento de los distintos procesos de tratamiento de datos, aspecto destacable que contrasta enormemente con el avance legislativo visible en España.

En lo que respecta a las obligaciones atinentes al ejercicio de las funciones del DPD, el artículo 50 numeral 7 de la LOPD manda que el mismo estará obligado a mantener la "más estricta" confidencialidad en el ejercicio de sus funciones. El presente articulado tiene como finalidad evitar que, por parte de quienes están en contacto con los datos personales almacenados en ficheros, se realicen filtraciones no consentidas por los titulares de los mismos.

Adicionalmente, se espera que la persona que desempeñe las atribuciones del DPD, ejecute de forma prolija sus actividades dentro de la institución tratante de datos personales, lo cual, es relevante indicar que, conforme a lo estipulado por la ya citada normativa, el DPD, en caso de incumplimiento de sus funciones deberá responder de forma administrativa, civil y penalmente conforme manda la ley.

2.2.2. Reflexiones sobre las funciones y obligaciones del Delegado de Protección de Datos, análisis comparativo Ecuador – España.

Una vez que hemos señalado las principales atribuciones y obligaciones del DPD en el marco normativo ecuatoriano, es necesario tomar en cuenta el punto de vista normativo y doctrinario español con la finalidad que acentuar lo mencionado.

En contraste con nuestra normativa, la legislación española amparada en instrumentos normativos como el Reglamento General de Protección de Datos Personales (en adelante RGPD) emitido por la Comisión de la Unión Europea (UE) 2016/679, la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (LOPDPDD) y el Reglamento de la Ley Orgánica de Protección de Datos de carácter personal, desarrolla los distintos aspectos a tomar en cuenta para la aplicación del cargo del Delegado de Protección de Datos (DPD) o también denominado Data Protection Officer (DPO), es así como el artículo 39 del RGPD establece las diversas funciones a ser ejecutadas por el DPD:

Ley de Protección de Datos Personales (2021)	**Reglamente General de Protección de Datos emitido por la Comisión de la Unión Europea (UE) 2016/679**
1) Asesorar al responsable, al personal del responsable y al encargado del tratamiento de datos personales, sobre las disposiciones contenidas en esta Ley, el	(a) to inform and advise the controller or the processor and the employees who

reglamento, las directrices, lineamientos y demás regulaciones emitidas por la Autoridad de Protección de Datos Personales	carry out processing of their [1]obligations pursuant to this Regulation and to other Union or Member State data protection provisions;
2) Supervisar el cumplimiento de las disposiciones contenidas en esta Ley, el reglamento, las directrices, lineamientos y demás regulaciones emitidas por la Autoridad de Protección de Datos Personales;	b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits
3) Asesorar en el análisis de riesgo, evaluación de impacto y evaluación de medidas de seguridad, y supervisar su aplicación;	(c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;
4) Cooperar con la Autoridad de Protección de Datos Personales y actuar como punto de contacto con dicha entidad,	(d) to cooperate with the supervisory authority

[1] Traducción oficial al español: "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 presente 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 presente Reglamento, de otras 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, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes; c) ofrecer el 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; d) cooperar con la autoridad de control; e) 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, y realizar consultas, en su caso, sobre cualquier otro asunto. 2. El delegado de protección de datos desempeñará 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." (RPGD, 2016)

con relación a las cuestiones referentes al tratamiento de datos personales; y,	
5) Las demás que llegase a establecer la Autoridad de Protección de Datos Personales con ocasión de las categorías especiales de datos personales	(e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter
	2. The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing

Tabla1. Elaboración propia (2023)

En primer lugar, debemos señalar que la normativa ecuatoriana, así como la española manda como primera función la de "asesoramiento", tanto de la normativa aplicable en materia de protección de datos personales como de la aplicación de la evaluación de impacto en los casos establecidos y, conforme lo especifica la ley ecuatoriana, adicionalmente, sobre la aplicación y supervisión de medidas de seguridad.

Acorde a lo manifestado debemos señalar que la Real Academia española define a la palabra "asesorar" como "dar consejo o dictamen sobre un asunto", en este caso sobre la aplicación en materia de protección de datos personales. De esta forma, entendemos que el DPD se establece como un ente complementario, su principal enfoque implica el fortalecimiento de las medidas de protección entorno al tratamiento de datos personales, por tal, es menester que el DPD posea un amplio espectro de comunicación con todos los implicados en el tratamiento de datos y sus directivos, así como un extenso conocimiento respecto de la normativa, actividades y operaciones que ejecuta la institución tratante de datos personales, aspectos que, como veremos más adelante, enmarcan un perfil necesario mas no expreso en la actual norma.

La Agencia Española de Protección de Datos, en desarrollo de los conceptos atenientes a la figura del DPD, nos menciona en su texto *"*Directrices sobre los delegados de Protección de Datos", que el Grupo de Trabajo del artículo 29 recomienda que el responsable del tratamiento busque el asesoramiento del DPD en las siguientes cuestiones, entre otras:

- Si debe llevarse a cabo o no una evaluación de impacto relativa a la protección de datos;
- qué metodología debe seguirse al llevar a cabo una evaluación de impacto;
- Si debe realizarse la evaluación de impacto en la propia organización o subcontratarse;
- Que salvaguardias (incluidas medidas técnicas y organizativas) deben aplicarse para mitigar cualquier riesgo para los derechos e intereses de los interesados;
- Si la evaluación de impacto relativa a la protección de datos se ha llevado a cabo correctamente o no y si sus conclusiones (si seguir adelante o no con el tratamiento y qué salvaguardias aplicar) son conformes con el RGPD. (AEPD, 2018, pp. 19-20)

A su vez menciona que en caso de que el Responsable del tratamiento de Datos (RT) considere oportuno la no aplicación del contenido expresado en el asesoramiento, este deberá motivar su decisión por escrito.

Una diferencia notable en contraste con nuestra legislación es que la normativa española agrega a esta primera función la responsabilidad de "informar". La RAE (s.f.) define al término "informar" como *"*enterar o dar noticia de algo", y es que como la normativa lo dispone, el DPD deberá informar a los implicados del tratamiento de datos de las obligaciones y disposiciones vigentes en torno a la protección de datos, sin embargo, el punto de vista español considera que la función de "informar" va más allá de lo estipulado, es así como la AEPD pone a consideración de las instituciones tratantes que será pertinente comunicar a los titulares, aspectos relativos al tratamiento de datos (normativa aplicable, método de tratamiento, etc.), finalidad del proceso, legitimación del tratamiento, destinatarios, derechos y su método de ejercerlos y la procedencia de los datos, así como de la información de contacto del responsable, al igual que del DPD.

Si bien se menciona que la entidad tratante de datos personales podrá informar en cualquier medio necesario, variable según la necesidad de quien solicita, se destaca que será esencial que dicho comunicado posea un lenguaje claro, sencillo, conciso, de fácil acceso y transparente. Por otro lado, no será necesario informar el interesado ya disponga

de la información, ni tampoco, en el caso de que los datos no procedan del interesado, cuando:

- La comunicación resulte imposible o suponga un esfuerzo desproporcionado;
- El registro o la comunicación esté expresamente establecido por el Derecho de la Unión o de los Estados miembros;
- Cuando los datos deban seguir teniendo carácter confidencial por un deber legal de secreto. (AEPD, 2018, p. 4)

Aunque nuestra legislación no considere de forma expresa tal desarrollo del término "informar" en el tratamiento de Datos personales, el capítulo VII, *del responsable, encargo y Delegado de Protección de Datos*, artículo 51, manifiesta el deber del RT de reportar y mantener actualizada la información ante la futura Agencia de Protección de Datos Personales (en adelante APDP) sobre:

1) Identificación de la base de datos o del tratamiento;
2) El nombre domicilio legal y datos de contacto del responsable y encargado del tratamiento de datos personales;
3) Características y finalidad del tratamiento de datos personales;
4) Naturaleza de los datos personales tratados;
5) Identificación, nombre, domicilio legal y datos de contacto de los destinatarios de los datos personales, incluyendo encargados y terceros;
6) Modo de interrelacionar la información registrada;
7) Medios utilizados para implementar los principios, derechos y obligaciones contenidas en la presente Ley y normativa especializada;
8) Requisitos y herramientas administrativas técnicas y físicas, organizativas y jurídicas implementadas para garantizar la seguridad y protección de datos personales;
9) Tiempo de conservación de los datos. (LOPDP, 2021, art.51)

Como pudimos matizar, si bien la norma ecuatoriana puntualiza como responsabilidad del RT el mantener actualizada información relevante al tratamiento, al igual que la normativa española, ¿es posible que el DPD pueda ejercer dicha función en el ecuador al considerar que su naturaleza es la de una figura nexus entre las partes implicadas en el tratamiento de datos personales?

Respecto de las actividades del DPD de "Supervisar", la RAE (s.f.) lo define como "ejercer la inspección superior en trabajos realizados por otros", es decir, el DPD será el responsable de controlar y vigilar el cumplimiento de la normativa vigente, siendo

indispensable la revisión de las políticas y procedimientos internos que sean acordes a los lineamientos y regulaciones vigentes en el país.

La AEPD desarrolló de manera puntual, en su texto institucional, sobre las directrices a ser aplicadas por la figura del DPD en las administraciones públicas, las principales funciones que cumple un DPD, enfocado en el sector público, de supervisor y asesor en materia de protección de datos, este podrá concretar sus funciones en los siguientes actividades citadas a continuación:

- Cumplimiento de principios relativos al tratamiento, como los de limitación de finalidad, minimización o exactitud de los datos
- Identificación de las bases jurídicas de los tratamientos
- Valoración de compatibilidad de finalidades distintas de las que originaron la recogida inicial de los datos
- Existencia de normativa sectorial que pueda determinar condiciones de tratamiento específicas distintas de las establecidas por la normativa general de protección de datos
- Diseño e implantación de medidas de información a los afectados por los tratamientos de datos
- Establecimiento de mecanismos de recepción y gestión de las solicitudes de ejercicio de derechos por parte de los interesados
- Valoración de las solicitudes de ejercicio de derechos por parte de los interesados
- Contratación de encargados de tratamiento, incluido el contenido de los contratos o actos jurídicos que regulen la relación responsable-encargado
- Identificación de los instrumentos de transferencia internacional de datos adecuados a las necesidades y características de la organización y de las razones que justifiquen la transferencia
- Diseño e implantación de políticas de protección de datos
- Auditoría de protección de datos
- Establecimiento y gestión de los registros de actividades de tratamiento
- Análisis de riesgo de los tratamientos realizados
- Implantación de las medidas de protección de datos desde el diseño y protección de datos por defecto adecuadas a los riesgos y naturaleza de los tratamientos
- Implantación de las medidas de seguridad adecuadas a los riesgos y naturaleza de los tratamientos

- Establecimiento de procedimientos de gestión de violaciones de seguridad de los datos, incluida la evaluación del riesgo para los derechos y libertades de los afectados y los procedimientos de notificación a las autoridades de supervisión y a los afectados
- Determinación de la necesidad de realización de evaluaciones de impacto sobre la protección de datos
- Realización de evaluaciones de impacto sobre la protección de datos
- Relaciones con las autoridades de supervisión
- Implantación de programas de formación y sensibilización del personal en materia de protección de dato. (AEPD, 2018, p. 4)

Es relevante destacar que entre las acciones que podrá ejecutar el DPD, desde el punto de vista español, en torno al cumplimiento de supervisión implicarían las siguientes:

- recabar información para determinar las actividades de tratamiento;
- analizar y comprobar la conformidad con la normativa de las actividades de tratamiento;
- informar, asesorar y emitir recomendaciones al responsable o al encargado del tratamiento" (Grupo De Trabajo Sobre Protección De Datos Del Artículo 29, 2018, p. 19)

Por último, mencionaremos que tanto nuestra normativa, al igual que la española, toman en consideración la función del delegado como punto de contacto entre la administración y sus administrados, no obstante, esta última amplía esta concepción por medio del artículo 38 numeral 6 del RGPD cuyo texto dispone:

> The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests. (RGPD, 2016)

Complementario a la norma *ut supra*, entre las posibles funciones adicionales a ejecutar por parte del DPD, la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales de España, determina en su artículo 37 los casos en que es necesaria la intervención del DPD por reclamación ante las autoridades de protección de datos:

> Intervención del delegado de protección de datos en caso de reclamación ante las autoridades de protección de datos.

1) Cuando el responsable o el encargado del tratamiento hubieran designado un delegado de protección de datos el afectado podrá, con carácter previo a la presentación de una reclamación contra aquéllos ante la Agencia Española de Protección de Datos o, en su caso, ante las autoridades autonómicas de protección de datos, dirigirse al delegado de protección de datos de la entidad contra la que se reclame.

   En este caso, el delegado de protección de datos comunicará al afectado la decisión que se hubiera adoptado en el plazo máximo de dos meses a contar desde la recepción de la reclamación.

2) Cuando el afectado presente una reclamación ante la Agencia Española de Protección de Datos o, en su caso, ante las autoridades autonómicas de protección de datos, aquellas podrán remitir la reclamación al delegado de protección de datos a fin de que este responda en el plazo de un mes.

   Si transcurrido dicho plazo el delegado de protección de datos no hubiera comunicado a la autoridad de protección de datos competente la respuesta dada a la reclamación, dicha autoridad continuará el procedimiento con arreglo a lo establecido en el Título VIII de esta ley orgánica y en sus normas de desarrollo.

3) El procedimiento ante la Agencia Española de Protección de Datos será el establecido en el Título VIII de esta ley orgánica y en sus normas de desarrollo. Asimismo, las comunidades autónomas regularán el procedimiento correspondiente ante sus autoridades autonómicas de protección de datos. (LOPDGDD, 2018, art.37)

Adicionalmente el artículo 65 numeral 4 del mismo cuerpo normativo señala:

> Antes de resolver sobre la admisión a trámite de la reclamación, la Agencia Española de Protección de Datos podrá remitir la misma al delegado de protección de datos que hubiera, en su caso, designado el responsable o encargado del tratamiento o al organismo de supervisión establecido para la aplicación de los códigos de conducta a los efectos previstos en los artículos 37 y 38.2 de esta ley orgánica. (LOPDGDD, 2018, art.65)

Lo interesante del presente artículo citado es la relevancia del delegado como un mecanismo de celeridad en los procesos de trámite de reclamación, si bien la legislación ecuatoriana no profundiza en las capacidades o lineamientos aptos para el DPD, se entiende que al otorgar su información de contacto y establecerse como una línea de comunicación directa en caso de reclamación es posible, al igual que España, acelerar el proceso de reclamación en el país.

2.2.3. Atribuciones especiales del Delegado de Protección de Datos.

Acorde a la normativa vigente se establece una serie de facultades especiales en favor del desempeño activo del DPD, cuyo cumplimiento y observancia deberán de ser ejecutadas por el Responsable (RT) y el Encargado (ET) del tratamiento de datos, es así como el artículo 50 de la LOPD manda:

> Para la ejecución de las funciones del delegado de protección de datos, el responsable y el encargado de tratamiento de datos personales, deberán observar lo siguiente:
>
> 1) Garantizar que la participación del delegado de protección de datos personales, en todas las cuestiones relativas a la protección de datos personales, sea apropiada y oportuna;
>
> 2) Facilitar el acceso a los datos personales de las operaciones de tratamiento, así como todos los recursos y elementos necesarios para garantizar el correcto y libre desempeño de sus funciones;
>
> 3) Capacitar y actualizar en la materia al delegado de protección de datos personales, de conformidad con la normativa técnica que emita la Autoridad de Protección de Datos Personales;
>
> 4) No podrán destituir o sancionar al delegado de protección de datos personales por el correcto desempeño de sus funciones;
>
> 5) El delegado de protección de datos personales mantendrá relación directa con el más alto nivel ejecutivo y de decisión del responsable y con el encargado;
>
> 6) El titular de los datos personales podrá contactar al delegado de protección de datos personales con relación al tratamiento de sus datos personales a fin de ejercer sus derechos; y,
>
> 7) El delegado de protección de datos personales estará obligado a mantener la más estricta confidencialidad respecto a la ejecución de sus funciones". (LOPDP, 2021, art.50)

El citado articulado busca garantizar el cumplimiento del rol del DPD como figura nexus entre la administración y sus administrados, esto implica la actualización continua y confidencial de la información propia de su profesión como también la seguridad laboral en el desempeño de sus funciones bajo los estándares pertinentes, para lo cual, es indispensable que la entidad tratante de datos impulse un proceso informativo que cuide y salvaguarde la veracidad del proceso.

Una cuestión a resaltar, con relación al presente articulado, es la necesidad de capacitar y actualizar en la materia de protección de datos al DPD, si consideramos que este conforma una instancia de control y asesoramiento respecto de los datos a tratar, debemos insinuar que el proceso informativo de la entidad tratante de datos recae en parámetros

internos respecto del proceso, volumen y tipo de datos que maneja, lo cual nuevamente se encuentra sin normar por falta de una autoridad competente.

Otro aspecto a destacar radica en la capacidad que tienen los titulares cuyos datos personales sean tratados por la entidad pública o privada, los cuales podrán contactar con el DPD a cargo en caso de requerirlo, aspecto compartido con la normativa española.

De igual forma, la figura del delegado como un ente que goza de independencia para actuar, considerando que su principal propósito es constituir un puente entre la administración y las organizaciones que ejecutan el tratamiento de datos, toma en cuenta una serie de facultades a las que se ven obligados a respetar los demás integrantes del tratamiento de datos personales.

Se prevé que el DPD goce de una participación activa en el proceso de tratamiento de datos personales disponiendo de toda la información y recursos pertinentes para el cumplimiento de sus funciones, ante lo cual, se debe destacar que si bien el DPD goza de una influencia considerable en el proceso de tratamiento de datos por cuanto se deberá garantizar el adecuado acceso a información relevante y pertinente en la ejecución de sus funciones, únicamente promueve la correcta aplicación de los procesos, no ejecuta el tratamiento de datos en cuestión, no obstante, nuestra normativa no establece una prohibición explicita para su participación, por tal entendemos que se encuentra a la discrecionalidad en la actualidad.

Adicional a la facultad de información, el DPD, mantiene un nivel de independencia lo cual, según Rosa García:

> Garantiza que no recibirá ninguna instrucción en lo que respecta al desempeño de sus funciones, no pudiendo ser destituido ni sancionado por su desempeño, y rindiendo cuentas al más alto nivel jerárquico de la organización'' (García, 2019)

Esto permite que la figura del DPD goce de un nivel de protección frente a posibles remociones o sanciones, salvo que se exista un incumplimiento justificado de sus funciones.

2.3. Obligatoriedad de nombrar un Delegado de Protección de Datos Personales

La LOPDP define al DPD como la persona natural cuya contratación será voluntaria u obligatoria por parte del Responsable (RT) y Encargado (ET) de datos personales, conforme lo establezca la normativa pertinente, siendo indispensable su presencia en los casos detallados en el artículo 48 del citado cuerpo normativo, señalados a continuación:

> 1) Cuando el tratamiento se lleve a cabo por quienes conforman el sector público de acuerdo con lo establecido en el artículo 225 de la Constitución de la República;
> 2) Cuando las actividades del responsable o encargado del tratamiento de datos personales requieran un control permanente y sistematizado por su volumen, naturaleza, alcance o finalidades del tratamiento, conforme se establezca en esta Ley, el reglamento a ésta, o en la normativa que dicte al respecto la Autoridad de Protección de Datos Personales;
> 3) Cuando se refiera al tratamiento a gran escala de categorías especiales de datos, de conformidad con lo establecido en el reglamento de esta Ley; y,
> 4) Cuando el tratamiento no se refiera a datos relacionados con la seguridad nacional y defensa del Estado que adolezcan de reserva ni fuesen secretos, de conformidad con lo establecido en la normativa especializada en la materia.
> La Autoridad de Protección de Datos Personales podrá definir nuevas condiciones en las que deba designarse un delegado de protección de datos personales y emitirá, a dicho efecto, las directrices suficientes para su designación. (LOPDP, 2021, art.48)

Ante el primer caso, debemos señalar que la normativa constitucional del 2008 en su apartado 225, reconoce como entidades que conforman el sector público y, por tanto, se encuentran obligadas a la contratación de un Delegado (DPD) son las siguientes:

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. (Constitución de la República del Ecuador, 2008, art.225).

En contraste con el presente articulado, la autoridad española ha preferido excluir a los tribunales pertenecientes a la función judicial y optó por desarrollar puntualmente sobre que instituciones, tanto públicas como privadas, deberán designar un DPD, sin perjuicio de su interés voluntario por nombrarlo:

> Los responsables y encargados del tratamiento deberán designar un delegado de protección de datos en los supuestos previstos en el artículo 37.1 del Reglamento (UE) 2016/679 y, en todo caso, cuando se trate de las siguientes entidades:
> a) Los colegios profesionales y sus consejos generales.

b) Los centros docentes que ofrecen 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 explotan redes y presentan servicios de comunicaciones electrónicas conforme a lo dispuesto en su legislación específica, cuando tratan habitualmente y sistemáticamente datos personales a gran escala.

d) Los prestadores de servicios de la sociedad de la información cuando elaboran una gran escala de 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 desarrollan actividades de publicidad y prospección comercial, incluidas 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.

Se exceptúan los profesionales de la salud que, aun estando legalmente obligados al mantenimiento de las historias clínicas de los pacientes, ejerzan su actividad a título individual.

m) Las entidades que tienen como uno de sus objetos la emisión de informes comerciales que pueden referirse a personas físicas.

n) Los operadores que desarrollan 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. (LOPDGDD, 2016, art.34)

Por otro lado, conforme lo establece el numeral segundo, es obligatoria la presencia del DPD, en general, para el control permanente y sistematizado de datos personales por parte del Encargado (ET) o Responsables (RT) debido al volumen, naturaleza, alcance y finalidades necesarias en su actividad. Aunque dicha necesidad está sujeta a las posibles determinaciones del aún faltante reglamento a la Ley Orgánica de Protección de Datos Personales, dejándonos un vacío hasta la presente fecha.

Desde el punto de vista español, será obligatoria la presencia de un DPD cuando exista un tratamiento de datos de forma, "*permanente y sistematizado"*. Pese a la falta de desarrollo en la ley respecto de que se entiende por estos términos, por medio de las Directrices emitidas por la AEPD (2016) se entiende como permanente o habitual lo siguiente: "continuado o que se produce a intervalos concretos durante un periodo concreto; recurrente o repetido en momentos prefijados; que tiene lugar de manera constante o periódica" (p. 9).

Por otro lado, se interpretará al término, sistemático, por medio de los siguientes significados: "que se produce de acuerdo con un sistema; preestablecido, organizado o metódico; que tiene lugar como parte de un plan general de recogida de datos; llevado a cabo como parte de una estrategia." (AEPD, 2016, p. 9)

Continuando con el apartado número tres, se hace énfasis en la importancia del DPD frente al tratamiento de datos en gran escala con relación a las categorías especiales de datos; la norma especializada hace referencia a dichas categorías en su artículo 25 y nos menciona que serán considerados como tales aquellos datos personales relacionados a niños, niñas y adolescentes; datos sobre la salud y cuando implique información de personas con discapacidad y de sus sustitutos; adicionalmente, como ya lo mencionamos anteriormente, el mismo apartado incluye a aquellos datos sensibles cuyo contenido hace referencia a información relacionada con:

> La etnia, identidad de género, identidad cultural, religión, ideología, filiación política, pasado judicial, condición migratoria, orientación sexual, salud, datos biométricos, datos genéticos y aquellos cuyo tratamiento indebido pueda dar origen a discriminación, atenten o puedan atentar contra los derechos y libertades fundamentales. (LOPDP, 2021, art.25)

Si bien tanto la normativa ecuatoriana como la española no puntualizan o definen explícitamente parámetros que determinen los distintos aspectos que conforman un tratamiento a "*gran escala*", la AEPD pone a consideración de las instituciones distintos umbrales a tomar en cuenta, tales como: la cifra de población implicada en el tratamiento (titulares); volumen de los datos a ser tratados; el alcance geográfico y la duración del

tratamiento de datos, al igual que, será necesario analizar si el tratamiento se encuentra enfocado a escala regional, nacional o supranacional.

Como es perceptible, la normativa citada hace énfasis en la relevancia de los datos sensibles al agregar un estricto grado de seguridad y procedimiento antes de su tratamiento por parte de las instituciones, estando prohibido su uso salvo excepción contemplada en el artículo 26 del mismo cuerpo normativo, previa autorización emitida por el titular o conforme lo estipule la ley. No obstante, es necesario recalcar que los parámetros en función del DPD aún se encuentra a la espera del reglamento a la ley y de la aún pendiente, hasta la fecha, nominación de la Autoridad de Protección de Datos, cuyo papel fomentará el control y desarrollo de la protección de datos en el país.

2.4. Sobre la Certificación del Delegado de Protección de Datos

Conforme a lo expuesto, desde el punto de vista ecuatoriano, entendemos al Delegado de Protección de Datos Personales (DPD) como aquella persona natural, cuyo cargo promueve la comunicación activa entre los integrantes del sistema de protección de datos personales y la Autoridad de Protección de datos personales, siendo su naturaleza la de velar por el correcto desempeño de las medidas y normas vigentes en materia de protección de datos personales, lo cual, promueve un sistema de comunicación directa con los titulares de datos personales, siendo sus funciones las de un asesor y supervisor de los mismos, una figura relevante en el proceso de tratamiento de datos de carácter personal, sin embargo, pese a lo mencionado, nuestra actual normativa no define o determina un perfil específico para la contratación de un DPD.

Nuestra normativa concibe la figura del DPD, sin establecer posibles requisitos como podrían ser: una determina profesión, experiencia, nivel de conocimiento, título o certificación, entre otros.

Ante la falta de desarrollo en nuestro país, a continuación, expondremos el proceso promovido por la normativa española sobre el uso de una certificación, notable diferencia con Ecuador, emitida por la denominada Autoridad de Protección de Datos española y su desarrollo entorno al entendimiento del perfil del DPD.

Entre los distintos aspectos que considera la normativa española en relación al mandato de la Comisión Europea, el DPD no tiene como requisito para su designación la titulación de una carrera específica u origen determinado dentro de la institución, es decir, entre las cualidades necesarias que deberá considerar el Encargado o Responsable del tratamiento de Datos para su contratación son: las bases profesionales y su conocimiento

en relación a las prácticas de tratamiento de datos y legislación en materia al igual que la capacidad para desempeñar sus funciones.

El RGPD adiciona su descripción al mencionar que dicho nivel de conocimiento deberá considerar el nivel de preparación especializada en función del volumen de las operaciones y de la protección exigida para la misma; ante ello se destacan las Directrices emitidas por la Autoridad de protección de datos sobre la aplicación del Reglamento Europeo de Protección de Datos (2017) el cual pone a consideración parámetros que nos permiten determinar un perfil profesional para el DPD:

> El primer punto a considerar es lo referente al *nivel de conocimiento y cualidades profesionales*, cuyo espectro abarca el entendimiento del sector societario, conocimiento administrativo, normativo y organizacional de las instituciones, y, en lo relativo al proceso y seguridad del tratamiento de datos. Véase que la contratación del DPD será una respuesta a la cantidad de datos a tratar por parte de una organización, puesto que las características de los datos, su sistematización o la transferencia de los mismos pueden variar. (REPD,2017)

Por último, en lo que respecta a la capacidad para desempeñar sus funciones, si bien es necesario considerar la inexistencia de posibles inhabilitaciones o impedimentos se recomienda discurrir sobre las cualidades personales con relación a la ética profesional del aspirante a DPD y su integridad, ya que trabajará en medio del resguardo de información de los titulares de datos.

Cabe resaltar que el Ecuador carece hasta la actualidad de directrices de estudio que analice estas cuestiones a diferencia de la administración española, es aquí donde podemos nuevamente insinuar que nuestra administración no concede un perfil específico de los criterios a los cuales deben atenerse los entes encargados del tratamiento de datos para la contratación de un delegado.

Uno de los aspectos más interesante que podemos encontrar en España sobre el perfil profesional de los Delegados de Protección de Datos (DPD) es su sistema de certificación autorizado por la AEPD en colaboración con La Entidad Nacional de Acreditación (ENAC), los cuales, en cumplimiento de la norma UNE-EN ISO/IEC 17024:2012, que regula sobre los sistemas de certificación internacionales, busca fomentar el adecuado perfil profesional de aquellos aspirantes al puesto de DPD.

Pese a que la norma no menciona la obligatoriedad de llevar dicha certificación, autores cono Susana Lozano (2018) considera que ‘‘los DPD certificados afrontarán las

oportunidades profesionales que ofrece el mercado con una situación más ventajosa, aportando mayor seguridad y garantías a las empresas que los contraten" (p.25).

Ya que el mecanismo de contratación de un Delegado, según la norma española, puede ser por contrato de trabajo o contrato de servicios es recomendable considerar al personal cuyo perfil profesional cuente con una certificación por cuanto otorga fiabilidad en la cualificación del desempeño profesional en sus funciones, llegando a considerarse una propuesta de mejora para la promoción de empleo, en tanto cualquier individuo externo o interno a la institución con capacitación puede suplir dicho cargo.

Aunque de forma general, mencionaremos que para acceder a este proceso de titulación se requiere cumplir un determinado número de horas de formación dependiendo de la experiencia y porcentaje de conocimientos en materia de protección de datos del aspirante. Una vez culminado el proceso de formación se procederá a una evaluación que constate el nivel de conocimiento para culminar en la inscripción:

Experiencia Profesional	**Cumplimiento de Horas de Formación**
5 años	No necesario
3 años	60 horas
2 años	100 horas
Sin experiencia	180 horas

Tabla 2. Elaboración propia (2023)

Destacamos este aspecto de España por cuanto no solo promulga la generación de delegados cuya principal función es el prolijo cumplimiento de prácticas orientadas a la protección de datos, también permiten la generación de instituciones de formación profesional, lo cual, hasta cierta medida reduce la carga administrativa de las autoridades encargadas de la protección de datos.

CONCLUSIONES Y RECOMENDACIONES

La Ley Orgánica de Protección de Datos Personales, en el Ecuador, trajo nuevos elementos prestos al desarrollo y aplicación de múltiples entidades cuyas actividades ejecutan el tratamiento de datos personales. El Delegado de Protección de Datos se configura en nuestro país como un nuevo perfil profesional encargado del control y asesoramiento a ser aplicado en el tratamiento de datos personales, una nueva propuesta de trabajo para el país.

Si bien es cierto que esta novedosa figura representa un nicho de oportunidades en un sector en crecimiento, su aplicación, conforme a la normativa actual, ha presentado diversos obstáculos que entorpecen o dificultan la correcta aplicación del mandato normativo. La falta del Reglamento a la Ley de Protección de Datos Personales y la designación de la Autoridad de Protección de Datos genera un desconcierto al momento de considerar la nominación de un DPD, puesto que la ausencia de parámetros o lineamientos generan un vacío en nuestra legislación, pese a que la disposición transitoria primera establece la vigencia del régimen sancionatorio a partir del 26 de mayo del presente año.

Si bien la figura del DPD se conceptualiza como aquella persona natural encargada de ejercer las funciones establecidas en la normativa en materia, cuyo rol principal se concentra principalmente en las de asesor y supervisor del tratamiento de datos personales ejercido por la entidad, se pone a consideración la perspectiva Europea cuyo punto de vista se extiende a las entidades jurídicas. Vinculado a la idea de mejorar y fomentar el adecuado proceso en el tratamiento de datos personales y ampliar las propuestas de laborales, entidades especializadas en protección de datos pueden facilitar el desempeño de las funciones del DPD al poder contar con un conjunto de criterios y opiniones, distinto al único criterio que conlleva un solo individuo.

Entre los puntos que deberá tomar en consideración para las futuras autoridades en materia, las distintas funciones actuales y futuras a ser desempeñadas por el DPD, tomando en perspectiva el punto de vista español, expresan la responsabilidad del DPD como medio de información y apoyo en situaciones de reclamo ante las autoridades de protección de datos, lo cual, fomenta la celeridad y la actuación oportuna en la administración. Pese a que nuestra normativa establece que el DPD servirá como punto nexo de información entre las entidades encargadas del tratamiento de datos y la administración, la confusión y poco desarrollo de la figura, respecto del material o contenido objeto de la aplicación de dichas funciones, pueden generar dificultades a la hora de ejecutar eficazmente los procesos en favor de sus titulares, por tal es necesario un pronunciamiento sobre la aplicación de las funciones del DPD y la posibilidad de ejercer apoyo en situaciones de reclamo como lo establece la normativa española.

Adicionalmente, uno de los puntos que más genera incertidumbre y se recomienda su puntual observación es respecto del proceso de contratación del DPD en las instituciones. Por un lado, entendemos que la presencia del DPD podrá ser obligatoria para las instituciones privadas si la escala del tratamiento de datos rebasa una determinada

cantidad en su volumen, finalidad, naturaleza entre otros, valores aún no determinados por la actual ley, además del interés voluntario de su nombramiento. Aunque el Delegado de Protección de datos carezca de un perfil determinado para su contratación, el modo de contratación y las especificaciones del mismo se apegarán al criterio objetivo de las partes, no obstante, es recomendable considerar los parámetros analizados por las Autoridades de Protección de Datos de España a fin de acatar el cumplimiento pleno de la norma hasta un futuro pronunciamiento de las Autoridades en materia.

Por el contrario, la normativa especializada establece la obligatoriedad del DPD en las instituciones detalladas en el artículo 225 de la Constitución de la República del Ecuador, ante lo cual se concluye que existe un problema con la norma al no establecer parámetros de contratación necesarios para la justificación del puesto laboral en cuestión, considerando que el artículo 226 de la norma constitucional establece que las instituciones del estado actúan solamente en virtud de lo establecido por la constitución y la ley, este vacío, en otras palabras, obstaculiza la actuación pública.

Si bien la LOPD no establece ni esclarece que factores determinan la idoneidad del profesional para ejecutar las funciones de DPD, al existir una obligatoriedad de la administración pública para el cumplimiento de la norma es posible tomar en consideración las distintas pautas y directrices emitidas por España, siendo necesario que las instituciones públicas conforme su discrecionalidad, debidamente motivada, y en favor de sus competencias puedan cumplir la norma establecida. Bajo esta misma lógica, se recomienda no considerar el uso de la figura de contratación por nombramiento por cuanto al existir una necesidad de desarrollo por parte de la administración pueden ocasionar inconvenientes a futuro.

Para finalizar, entendemos que el Ecuador ha puesto en marcha un proceso normativo cuyo eje principal gira entorno a los tiempos modernos, en una sociedad cada vez más interesada en la privacidad de los ciudadanos la Ley Orgánica de Protección de Datos Personales nace como un mecanismo de protección para el ejercicio de derechos de los titulares de datos personales, no obstante, pese al tiempo transcurrido aún nos encontramos en las primeras fases de una ley que deberá otorgar soluciones y respuestas a los vacíos presentados hasta la actualidad.

REFERENCIAS BIBLIOGRÁFICAS

Asamblea Nacional del Ecuador. *Código Orgánico de Integración Penal* (ley 0). RO. Suplemento 180 de 10 de febrero de 2014.

Asamblea Nacional del Ecuador. *Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos*. (Ley 67). R.O Suplemento 557 del 17 de abril de 2002.

Asamblea Nacional del Ecuador. *Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional.* R.O Suplemento 52 del 22 de octubre de 2009.

Asamblea Nacional del Ecuador. *Ley Orgánica de Protección de Datos Personales*. (ley 0) R.O Suplemento 472 del 14 de junio de 2021.

Asamblea Nacional del Ecuador. *Ley Orgánica del Sistema Nacional de Registro de Datos Públicos.* R.O Suplemento 162 del 31 de marzo de 2010.

Asamblea Nacional del Ecuador. *Ley Orgánica de Transparencia y Acceso a la Información Pública.* R.O Suplemento 245 del 7 de febrero del 2023.

Carrillo, F. (2021). *Los ejes centrales de la protección de datos: consentimiento y finalidad. Críticas y propuestas hacia una regulación de la protección de datos personales en Ecuador.* Recuperado de https://doi.org/10.18272/ulr.v8i1.2184

Constitución de la República del Ecuador [Const.]. (2008). 2da Ed. CEP Corte Constitucional del Ecuador. (3 de junio de 2015). Sentencia No. 182-15-SEP-CC.

Corte Constitucional del Ecuador. (22 de julio de 2020) Sentencia No. 1868-13-EP/20.

Corte Constitucional del Ecuador (15 de marzo de 2021). Sentencia No. 2064-14-EP/21.

Cortes Generales de España. *Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales.* D.O BOE.A-2018-16673 del 21 de noviembre de 2018.

Cortes Generales de España. *Reglamento Europeo de Protección de Datos.* D.O UE 2016 779 del 25 de mayo de 2018.

Durán, F. (2017*). Big data aplicado a la mejora de los servicios públicos y protección de datos personales*. Recuperado de: https://www.jacobea.edu.mx/revista/numero12.php

Lozano, S. (2018*). Delegado de Protección de Datos, el profesional más buscado*. Recuperado de https://revista.aenor.com/340/delegado-de-proteccion-de-datos-el-profesional-mas-buscado.html

Naranjo, L. (2021). *El dato personal como presupuesto del derecho a la protección de datos personales y del hábeas data en Ecuador*. Recuperado de https://revistas.uasb.edu.ec/index.php/foro/article/view/501/2419

Ordóñez, L. (2017). *La protección de datos personales en los estados que conforman la Comunidad Andina: estudio comparado y precisiones para un modelo interamericano de integración*. Recuperado de: https://repositorio.uasb.edu.ec/bitstream/10644/5947/1/07-TC-Ordo%c3%b1ez.pdf

Real Academia Española (s.f.). *Informar*. Recuperado de https://dle.rae.es/informar

Real Academia Española (s.f.). *Supervisar*. Recuperado de https://dle.rae.es/supervisar?m=form

Santamaría, F. (2020). *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.* Madrid, España: Derecho PUCP

BIBLIOGRAFIA

Agencia Española Protección De Datos. (2022). *La AEPD aprueba el primer código de conducta sectorial desde la entrada en vigor del Reglamento de Protección de Datos. Recuperado de:* https://www.aepd.es/es/prensa-ycomunicacion/notas-de-prensa/aepd-aprueba-primer-codigo-conducta-sectorial-desdeentrada-vigor-rgpd

Andonegui, M. (2005). *Evolución histórica de los sistemas ERP: de la gestión de materiales a la empresa digital.* Quito, Ecuador: Revista de Dirección y Administración de Empresas.

Arenas, M. (2006). *El derecho fundamental a la protección de datos personales en Europa*. Valencia, España: Tirant lo Blanch.

Bilbao, J. (1997). *La eficacia de los derechos fundamentales frente a los particulares. Análisis de la jurisprudencia del Tribunal Constitucional.* Madrid, España: CEPC.

Burzaco, M. (2020). *Protección de datos personales. Esquemas*. Madrid, España: Dykinson, S.L.

Cabanellas, G. (1981). *Diccionario de Derecho Usual.* Buenos Aires, Argentina: Editorial Heliasta.

Cabero, J. (2006). *Nuevas Tecnologías Aplicadas a la Educación.* Barcelona, España: McGraw-Hill Interamericana de España.

Campos, M. (2018). *La política de seguridad en el RGPD. Análisis de riesgos y Evaluación de Impacto*. Madrid, España: Wolters Kluwer.

Castellano, P. (2018). *El desempeño de las funciones del Delegado de Protección de Datos. Gestión de procesos críticos y casos prácticos.* Madrid, España: Bosch.

García, J (2011). *Derecho a la Intimidad Personal y Familiar*. Recuperado de: http://www.derechoecuador.com/articulos/detalle/archive/doctrinas/derechocivil/ 2011/02/02/derecho-a-la-intimidad-personal-y-familiar

Gonzales, L. (2019). *Control de nuestros datos personales en la era del big data: el caso del rastreo web de terceros*. Bogotá, Colombia: Estudios. SocioJurídicos. Recuperado de: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S012-579201

Grupo De Trabajo Sobre Protección De Datos Del Artículo 29. (2016). *Directrices sobre los delegados de protección de datos (DPD)* Recuperado de: https://aepd.es/sites/default/files/2019-09/wp243vol01-es.pdf

Jiménez, A y García, D (2020*). Evolución histórica del cumplimiento de la normativa de protección de datos en hospitales públicos de España*. Recuperado de: http://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1988348X2020000100014&lng=es&tlng=es.

Jiménez, P. (2001). *Antecedentes legislativos de la nueva Ley Orgánica de Protección de Datos Personales.* Madrid, España: La Ley.

Jorge, B. (2020). *El Principio De Diligencia Como Garantía De Justicia.* Recupero de: http://saberyjusticia.edu.do/index.php/SJ/article/view/51.

López, D. (2014*). Protección de datos y habeas data: una visión desde Iberoamérica.* Madrid, España: Agencia Española de Protección de Datos.

Lorica, B. (2013). *Data Analysis: Just One Component of The Data Science Workflow*. Estados Unidos: O'Reilly Inc.

Naranjo, L. (2021). *El dato personal como presupuesto del derecho a la protección de datos personales y del hábeas data en Ecuador*. Recuperado de https://revistas.uasb.edu.ec/index.php/foro/article/view/501/2419

Pérez, G. (2013). *Naturaleza Jurídica del Habeas Data*. Bogotá, Colombia: VC Editores y ACDPC.

Polo, A. (2022). *Privacidad, intimidad y protección de datos: una mirada estadounidense y europea. Recuperado de:* https://doi.org/10.20318/dyl.2022.6884

Rafael, V. (1993). *Protección Jurídica a la Protección de los Datos Personales Automatizados.* Madrid, España: Editorial Colex

Rodríguez, A. (2018*). Un Nuevo Orden Para Proteger Los Datos Personales*. Recuperado de: Dialnet-UnNuevoOrdenParaProtegerLosDatosPersonales-7258819.pdf

Rubio, F. (1993). *La forma de poder (Estudios sobre la Constitución)*. Madrid, España; Centro de Estudios Constitucionales.

Ruiz, C. (1994). *Entorno a la Protección de los Datos Personales Automatizados.* Madrid, España: Editorial Complutense.

Saiz, A. (2005). *De primacía, supremacía y derechos fundamentales en la Europa integrada: la declaración del Tribunal Constitucional de 13 de diciembre de 2004 y el Tratado por el que se establece una Constitución para Europa.* Madrid, España: CEPC.

Santamaría, F. (2020). *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.* Madrid, España: Derecho PUCP

Ugartemendia, J. y Ripol, S. (2017) *El Tribunal Constitucional en la encrucijada europea de los Derechos Fundamentales. Un análisis a partir del asunto Melloni y sus implicaciones*. Madrid, España.

Valdés, F. (1992). *Poderes del empresario y derechos de la persona del trabajador.* Madrid, España: Trotta.

Villaverde, I. (2006). *La jurisprudencia del Tribunal Constitucional sobre el derecho fundamental a la protección de datos personales.* Madrid, España: Ediciones Cinca.

Widow, F. (2015). *La ley de Hume en Hume: la discusión de la interpretación analítica de Treatise II*I. Recuperado de: https://revistas.ucm.es/index.php/ASHF/article/view/49971

Hill Interamericana de España.