DERECHO CRÍTICO: REVISTA JURÍDICA, CIENCIAS SOCIALES Y POLÍTICAS
Vol. 7, Núm. 7, 2025 (1-21)
ISSN: 2953 - 6464
DOI: https:/10.53591/dcjcsp.v7i7.2572

El delegado de protección de datos frente a los derechos y libertades de los ciudadanos en la legislación ecuatoriana

The Data Protection Officer Versus the Rights and Freedoms of Citizens in Ecuadorian Legislation

Jaime Lenin Hurtado Angulo

Derecho Crítico: Revista Jurídica Ciencias Sociales y Políticas
Fecha de recepción: 11/02/2025
Fecha de aceptación:15/3/2025

DERECHO CRÍTICO: REVISTA JURÍDICA, CIENCIAS SOCIALES Y POLÍTICAS
Vol. 7, Núm. 7, 2025 (1-21)
ISSN: 2953 - 6464
DOI: https:/10.53591/dcjcsp.v7i7.2572

El delegado de protección de datos frente a los derechos y libertades de los ciudadanos en la legislación ecuatoriana

The Data Protection Officer Versus the Rights and Freedoms of Citizens in Ecuadorian Legislation

Jaime Lenin Hurtado Angulo, PhD.[1]

Como citar: Hurtado Angulo, J. (2025) El delegado de protección de datos frente a los derechos y libertades de los ciudadanos en la legislación ecuatoriana. Derecho Crítico: Revista Jurídica, Ciencias Sociales y Políticas. 7(7) 1-21. DOI:10.53591/dcjcsp.v7i7.2572

Resumen: El artículo analiza el rol del Delegado de Protección de Datos (DPD) en Ecuador tras la entrada en vigor (2021) de la Ley Orgánica de Protección de Datos Personales (LOPDP), cuyo objetivo es garantizar los derechos y libertades fundamentales de los ciudadanos frente al tratamiento de sus datos personales. A través de una metodología jurídico-dogmática y cualitativa, se examinan los conceptos de datos personales y sensibles, los actores del tratamiento y la autoridad de control. Se destaca que el DPD asesora y supervisa el cumplimiento de la normativa. Sin embargo, su implementación enfrenta desafíos como la falta de cultura jurídica de la población, escasa formación profesional en materia de protección de datos y una autoridad de control con limitada independencia. Se concluye que el DPD es clave para una gestión ética de datos, pero su impacto efectivo requiere formación, conciencia ciudadana y un marco institucional sólido y autónomo.

Palabras clave: Datos personales; delegado de protección de datos; responsabilidad proactiva

Abstract: This article analyzes the role of the Data Protection Officer (DPO) in Ecuador following the entry into force (2021) of the Organic Law on Personal Data Protection (LOPDP). The LOPDP aims to guarantee the fundamental rights and freedoms of citizens concerning the processing of their personal data. Using a legal-dogmatic and qualitative

[1] Doctor en Ciencias Jurídicas (PhD) por la Comisión Nacional de Grados científicos - Universidad de La Habana, Magíster en Derecho Procesal, Magíster en Protección de Datos, especialista en Propiedad Intelectual, docente titular de la Universidad Católica de Santiago de Guayaquil (23 años) TIC aplicadas a la investigación jurídica. Autor de libros: Manual de Derecho Informático y la Prueba electrónica en el COGEP. https://orcid.org/0000-0001-9581-7651; Jaime.hurtado@cu.ucsg.edu.ec

ISSN: 2953 - 6464
DOI: https:/10.53591/dcjcsp.v7i7.2572

methodology, the article examines the concepts of personal and sensitive data, the actors involved in data processing, and the control authority. It highlights that the DPO advises on and supervises compliance with data protection regulations. However, its implementation faces challenges such as a lack of legal culture among the population, limited professional training in data protection, and a control authority with restricted independence. The article concludes that the DPO is crucial for ethical data management, but its effective impact requires training, citizen awareness, and a robust and autonomous institutional framework.

Keywords: Personal data; data protection officer; proactive responsibility

INTRODUCCIÓN

En el Ecuador, la protección de los datos personales ha tomado especial relevancia con la implementación de la Ley Orgánica de Protección de Datos Personales, LOPDP, que busca alinear el país con estándares internacionales en materia de privacidad y seguridad de la información. Esta normativa, inspirada en principios como los del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y el por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos RGPD), reconoce el derecho de las personas a controlar su información personal y establece obligaciones claras para las entidades que la procesan. En este contexto, el Delegado de Protección de Datos, DPD, se erige como una figura fundamental, responsable de supervisar el cumplimiento de la ley, asesorar a las organizaciones y actuar como enlace entre estas y los ciudadanos. Su labor es crucial para prevenir vulneraciones y garantizar que los derechos de los titulares de los datos personales se ejerzan efectivamente.

Sin embargo, el despliegue de esta figura enfrenta desafíos en el ámbito ecuatoriano, donde muchas instituciones aún están adaptándose a las exigencias de la LOPDP. La falta de cultura en protección de datos, la escasez de profesionales especializados y las particularidades del marco legal local —como las excepciones para entidades públicas o el tratamiento de datos

ISSN: 2953 - 6464
DOI: https:/10.53591/dcjcsp.v7i7.2572

sensibles— plantean obstáculos para una implementación óptima del rol del DPD. A pesar de ello, su correcta designación y operatividad pueden marcar la diferencia en la construcción de un ecosistema digital más seguro y transparente.

Finalmente, el impacto del DPD trasciende el ámbito técnico-jurídico, pues contribuye a fortalecer la confianza de la ciudadanía en el uso de tecnologías y servicios digitales. En un mundo donde los datos son un activo valioso, su gestión ética y responsable se convierte en un pilar para el ejercicio de otros derechos fundamentales, como la libertad de expresión, la no discriminación y la autodeterminación informativa. El caso ecuatoriano refleja, así, un avance significativo en la protección de las libertades individuales, aunque aún queda camino por recorrer en materia de concientización, capacitación y aplicación efectiva de la normativa. En este trabajo analizaremos el impacto del DPD en la defensa de los derechos fundamentales, explorando sus funciones, desafíos y contribución al equilibrio entre innovación tecnológica y protección de las libertades individuales. Para alcanzar los objetivos que nos proponemos, usaremos el método jurídico – dogmático, en el marco de una investigación cualitativa y se propone la siguiente pregunta de investigación:

¿Cómo contribuye la figura del delegado de protección de datos (DPD) a la garantía de los derechos fundamentales y al cumplimiento del principio de responsabilidad proactiva en el tratamiento de datos personales en el marco de la Ley Orgánica de Protección de Datos Personales del Ecuador?

Los datos personales

Podemos desagregar la expresión datos personales conceptualizando, en primer lugar, la expresion datos. Lo hacemos indicando que estos son toda letra, dígito, color, situación de hecho que, teniendo escaso contenido comunicacional, es decir, al proponerse a distintas personas, pueden ser interpretados de distinta forma y al ser sometido a un proceso o tratamiento, se convierte en información. En consecuencia, los datos constituyen el insumo desde donde se obtiene información.

ISSN: 2953 - 6464
DOI: https:/10.53591/dcjcsp.v7i7.2572

Por otra parte, aquellos datos que identifican a una persona natural o la hacen identificable, son los que se conocen como datos personales. (Davara, 2021) realiza la distinción indicada expresando:

> Un dato es una noticia cierta sobre un hecho. Informar es enterar o dar noticia de algo —es un testimonio que permite llegar al conocimiento de algo—, e información es la acción y efecto de informar. La información es el propio dato asociado a un fin determinado. El dato, como ya hemos indicado, puede cambiar la interpretación que se haga de la información.

En relación con el alcance del concepto de dato personal, habíamos afirmado previamente que estos incluyen todos aquellos datos que identifican a una persona natural o la hacen identificable. El nombre de una persona, su número de cédula de identidad, por solo mencionar estos, identifican a una persona natural; mientras que su información genética o la dirección IP[2] de alguno de sus dispositivos electrónicos, la hace identificable. (Álvarez, 2020) define los datos personales haciendo una enumeración abierta de los datos que pueden identificar o hacer identificable a una persona natural:

> Supone una novedad la consideración de dato personal a la vinculación de identificadores que hagan a una persona física identificable. Por tanto, son considerados como tales, los datos identificativos de las personas (como, por ejemplo, el nombre y apellidos, la dirección, el número del teléfono, la firma manuscrita, etcétera); los datos acerca de las características personales o las circunstancias sociales (como, por ejemplo, estado civil, edad, aficiones, pertenencia a asociaciones, etcétera); los datos académicos y profesionales; los datos relacionados con el empleo (profesión, puestos de trabajo, historial del empleado, etcetera); la información comercial, económica, financiera y de seguros (por ejemplo, un número de cuenta corriente, las deudas que se mantienen frente al responsable del fichero); la relativa a

[2] *Internet Protocol*: Protocolo de comunicación que permite identificar y enviar datos entre dispositivos en una red mediante direcciones numéricas (ej. 192.168.1.1). Es fundamental para el funcionamiento de Internet.

ISSN: 2953 - 6464
DOI: https:/10.53591/dcjcsp.v7i7.2572

> transacciones comerciales prestadas o recibidas; las fotografías y las imágenes obtenidas a través de cámaras de vídeo vigilancia, entre otras.

Ahora bien, no todos los datos personales tienen la misma connotación, es decir, algunos como el nombre, la profesión, la dirección domiciliaria, están vinculados a lo que se podría denominar: la esfera pública de las personas (datos personales públicos), mientras que otros, tales como: el estado de salud, la confesión religiosa, la filiación política o el estatus migratorio, están relaciondos a la intimidad de las personas (datos personales privados). A estos últimos se les reconoce la pertenencia a los denominados datos sensibles o de categorías especiales. La Ley Orgánica de Protección de Datos Personales define los datos sensibles:

> Datos relativos a: 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).

Sobre los datos sensibles, la propia Constitución de la República del Ecuador, CRE, establece en su art. 66.11, que nadie estará obligado a proporcionarlos en contra de su voluntad:

> Se reconoce y garantizará a las personas: […] 11. El derecho a guardar reserva sobre sus convicciones. Nadie podrá ser obligado a declarar sobre las mismas. En ningún caso se podrá exigir o utilizar sin autorización del titular o de sus legítimos representantes, la información personal o de terceros sobre sus creencias religiosas, filiación o pensamiento polí(Ley Orgánica de Protección de Datos Personales, s. f.)tico; ni sobre datos referentes a su salud y vida sexual, salvo por necesidades de atención médica (CRE, 2008).

Hemos indicado, con reiteración, que los datos, en general y, los datos personales, en particular, deben ser sometidos a tratamiento para transformarse en información. La expresión tratamiento tiene muchas acepciones, la que nos atañe la encontramos en la

ISSN: 2953 - 6464
DOI: https:/10.53591/dcjcsp.v7i7.2572

definición que propone el art.. 4 de la ley de la materia (Ley Orgánica de Protección de Datos Personales, s. f.):

> Tratamiento: 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.

Como se puede advertir, prácticamente cualquier acción que se desarrolle sobre los datos personales constituye tratamiento, no limitándose a procesos automatizados, el tratamiento puede ser realizado también mediante procedimientos no automatizados.

El derecho a la protección de datos personales.

Los datos personales, tal como los hemos conceptualizado, no siempre requirieron protección. En realidad, es el avance tecnológico el que se erigió como una amenaza de gran magnitud frente a los datos personales, lo que originó el sistema de protección que garantizara el pleno respeto a los derechos y libertades de las personas. Si bien es cierto que, aisladamente hubo intentos de proteger la intimidad, la reputación, el honor y derechos similares de las personas, no fue sino hasta finales del siglo XIX, que se empezó a estructurar el derecho a la protección de datos personales. Samuel Warren y Louis Brandeis, fueron los que estructuraron, en su célebre artículo *Right to Privacy*, en la *Harvard Law Review*, essto es, la revista de Derecho de esa universidad, lo que denominaron: derecho a ser dejado en paz (*right to be let alone*). Podríamos resumir la teoría antes referida expresando:

1. La privacidad se define como el derecho a vivir sin intrusiones injustificadas en la esfera personal, especialmente por parte de la prensa o terceros no autorizados.

ISSN: 2953 - 6464
DOI: https:/10.53591/dcjcsp.v7i7.2572

2. Argumentaban que la exposición no autorizada de aspectos íntimos (como cartas, imágenes u otros detalles personales) debía ser considerada un agravio legal, incluso si la información divulgada era cierta.
3. Aunque no existía un derecho explícito a la privacidad en la época, Warren y Brandeis lo asimilaron a principios jurídicos preexistentes, como la protección contra el *breach of confidence* (violación de confidencialidad) y los derechos de propiedad sobre las propias ideas y creaciones
4. No todo lo que ocurre en la vida de una persona es de interés público; ciertos aspectos merecen protección legal contra la divulgación indiscriminada, es decir, información perteneciente a la esfera de la intimidad personal.

Transcurrido más de un siglo despues de que la teoría de protección de datos de Warren y Brandeis se publicara, sus elementos esenciales, particularmente cuando se afirma que la protección de la información relacionda con la esfera íntima de las personas, compromete sus derechos y libertades, tienen plena vigencia aun en entornos digitales como aquellos en los que nos desarrollamos en la actualidad.

Elementos subjetivos de la protección de datos

Titular (interesado)

Es la persona natural que identifican los datos personales o la hacen identificable. Debemos recordar que una persona es tal, desde que es sujeto de derechos. El art. 60 del Código Civil dispone: “El nacimiento de una persona fija el principio de su existencia legal, desde que es separada completamente de su madre […]” (CC, 2005). Por otro lado, el art. 64 ibídem, determina: “La persona termina con la muerte” (CC, 2005).

De lo establecido en la legislación civil ecuatoriana, podemos sin dificultad inferir que la protección de los datos se reconoce a los sujetos de derechos, es decir, a quien ha nacido y mientras viva. Sin perjucio de lo previamente afirmado, los derechos inherentes a las personas fallecidas en relación son sus datos personales, pueden ser ejercidos por sus derechohabientes, salvo que el propio causante haya dispuesto expresamente lo que se deberá

ISSN: 2953 - 6464
DOI: https:/10.53591/dcjcsp.v7i7.2572

hacer con sus datos personales después de su fallecimiento, en lo que se denomina testamento digital[3].

Debemos indicar, que la definición de datos personales insiste en la limitación del alcance de su ambito, a las personas físicas o naturales, es decir, hay expresa exclusión, de tal ámbito de protección, a las personas jurídicas. "[…] las personas jurídicas están expresamente excluidas de la protección de la norma. Por ello, las sociedades, asociaciones, corporaciones y fundaciones a los que se refiere el art. 35 CC, no gozarán de ninguna de las garantías establecidas en el RGPD […]" (Aparicio & Vidal, 2019).

Finalmente, es necesario mencionar que la protección de los datos personales no abarca al tratamiento realizado en actividades familiares o domésticas, así se dispone en el art. 2 de la LOPDP. Tal exclusión se justifica en la medida que, pese a que el derecho a la protección de datos es autónomo, se enmarca en los mecanismos de protección de la intimidad, la privacidad, de intromisiones de terceros. Cuando se trata de actividades familiares o domésticas, el tratamiento de datos que se pudiera realizar se entiende realizado en un ámbito familiar que, como tal, se ampara en la confianza que genera dicho entorno. Sobre esta excepción (Megías, 2021) explica:

> La justificación de la excepción se encuentra con el fin último perseguido por la regulación, salvaguardar el control sobre los datos de carácter personal y el derecho a la vida privada y familiar de todo cicudadano. Pero serîa ilógico —o cuando menos parternalista— que, con esta intención, se impusieran obligaciones de control sobre uno mismo en relación a los datos generados en la esfera personal, familiar o de amistad, de ahí que estas actividades sean excluidas del ámbito de aplicación.

A nuestro entender, la aplicación de esta excepción está en directa relación con la cantidad de personas que puedan acceder a la información generada en actividades familiares o

[3] El testamento digital es un documento legal o conjunto de directivas que establece qué debe hacerse con los activos y presencia digital de una persona después de su fallecimiento. Evita conflictos legales, protege la privacidad del fallecido y facilita a los familiares el manejo de su herencia digital. Se recomienda integrarlo al testamento tradicional o formalizarlo con un notario.

ISSN: 2953 - 6464
DOI: https:/10.53591/dcjcsp.v7i7.2572

domésticas. Imagínese que, en una reunión familiar, se toman fotografías que luego, como de costumbre, son subidas a alguna red social. Si la cuenta de la red social mediante la cual se está compartiendo las imágenes se ha configurado de tal manera que solo aquellas personas que se han definido como "contactos" del titular de la cuenta de la red social tengan acceso a ellas, se aplicaría la excepción doméstica, pero si se trata de una cuenta pública, vale decir, sin restricciones de acceso, en tal caso, no se podría invocar tal excepción, por la cantidad personas que ecentualmente podrían tener acceso a la información (fotografías).

Responsable de tratamiento

Se designa como responsable a aquella persona natural o jurídica que determina el cómo y el para qué se realizará el tratamiento de los datos personales. La legislación ecuatoriana define al responsable como: "Persona natural o jurídica, pública o privada, autoridad pública, u otro organismo, que solo o conjuntamente con otros decide sobre la finalidad y el tratamiento de datos personales" (LOPDP, 2021). Es sin duda una de las figuras centrales, en la medida que asume las consecuencias legales de la posible afectación a los derechos y libertades de los titulares, que se pudieran producir durante el tratamiento de los datos personales. Al respecto, es opinión de (Hernández, 2021):

> Con independencia de su naturaleza o forma jurídica, el responsable es quien ejerce control sobre las decisiones que afectan los elementos fundamentales del tratamiento de datos, como son los fines y medios esenciales. Pueden considerarse como tales, el tipo y categoría de datos, o la duración del procesamiento, pero no la determinación del software utilizado para la implementación de un modelo de análisis de datos.

Es ante el responsable que el titular de los datos personales podrá ejercer sus derechos y es quien, en principio, lo resarcirá por los daños que ocasione un tratamiento de datos personales, si se comprueba que no ha actuado con la proactividad que le exije el art. 52 de la LOPDP.

ISSN: 2953 - 6464
DOI: https:/10.53591/dcjcsp.v7i7.2572

Encargado del tratamiento

El encargado del tratamiento es la persona natural o jurídica que, por cuenta y control del responsable, realiza el tratamiento de los datos personales. La LOPDP define esta figura de la siguiente forma: "Persona natural o jurídica, pública o privada, autoridad pública, u otro organismo que solo o conjuntamente con otros trate datos personales a nombre y por cuenta de un responsable de tratamiento de datos personales" (LOPDP, 2021). El art. 47.10 de la LOPDP dispone que entre el responsable y encargado debe existir una relación contractual que establezca la forma en que el encargado del tratamiento realice los procesos establecidos por el responsable, lo indica expresando:

> El responsable del tratamiento de datos personales está obligado a: […] 10) Suscribir contratos de confidencialidad y manejo adecuado de datos personales con el **encargado** y el personal a cargo del tratamiento de datos personales o que tenga conocimiento de los datos personales. (LOPDP, 2021)

Es importante indicar que siempre será el responsable del tratamiento de los datos quien determine la necesidad de acudir a un tercero (el encargado) que realice el tratamiento, sin perjuicio de aumir las consecuencias de un defectuoso cunplimiento de las obligaciones por parte del encargado, que puedan afectar los derechos y libertades del titular de los datos personales.

Destinatario

Como afirmamos *supra*, los datos procesados se convierten en información y esta sera la base para la toma de decisiones. La persona que debe tomar decisiones o la habilitada para el uso derivado de tal procesamiento es el destinatario.

> En el ámbito de la protección de datos, el término «destinatarios en protección de datos» se refiere a las personas físicas o jurídicas, entidades u organismos que reciben datos personales de parte de un responsable del tratamiento. Los destinatarios pueden ser terceros ajenos a la organización del responsable del tratamiento. Según el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, los

ISSN: 2953 - 6464
DOI: https:/10.53591/dcjcsp.v7i7.2572

> destinatarios pueden utilizar los datos personales exclusivamente para los fines específicos para los cuales se les han comunicado. (*¿Qué Son Los Destinatarios?*, 2025)

Como queda claro, el destinatario es aquella persona natural o jurídica a quien se le comunican los datos personales, para que los someta a tratamiento en los términos que autónomamente determine, lo que lo diferencia del encargado de protección de datos. En la legislación de la Unión Europea, UE, en materia de protección de datos, se propone una distinción entre estos dos agentes del sistema de protección de datos:

> Según el RGPD (art. 4.8 RGPD), encargado de tratamiento (ET) es la entidad que trata datos personales por cuenta del responsable del tratamiento (RT). En principio y conforme a esta definición, todas las entidades contratadas por un RT para que les preste un servicio que precise tratar datos personales responsabilidad del RT serían ET, ya que todas realizan el tratamiento por encargo y por cuenta del RT.
>
> Del mismo modo el art. 4.9 RGPD define a los destinatarios como aquella entidad a la que un RT o un ET les cedan o comuniquen datos personales.
>
> Por lo tanto, estaremos ante un encargo del tratamiento cuando la entidad que nos presta el servicio está tratando los datos personales por nuestra cuenta, o sea siguiendo únicamente nuestras instrucciones (art. 28.3.a RGPD). En cambio, estaremos ante una cesión de datos cuando la entidad que nos presta el servicio está tratando los datos personales por su cuenta, o sea sin seguir nuestras instrucciones. (Legal, 2022)

De más está decir que, tanto el encargado como el destinatario deben sujetarse a la finalidad del tratamiento establecido por el responsable, en el desarrollo de las actividades de tratamiento a la que sometan los datos personales que se les haya comunicado. Todo lo anterior se ha reconocido en el art. 33 de la LOPDP

> Los datos personales podrán transferirse o comunicarse a terceros cuando se realice para el cumplimiento de fines directamente relacionados con las funciones legítimas del responsable y del destinatario, cuando la transferencia se encuentre configurada

ISSN: 2953 - 6464
DOI: https:/10.53591/dcjcsp.v7i7.2572

> dentro de una de las causales de legitimidad establecidas en esta Ley, y se cuente, además, con el consentimiento del titular. (LOPDP, 2021)

Autoridad de protección de datos

La legislación en materia de protección de datos personales establece que debe existir un órganismo independiente que supervise la correcta aplicación de las normas aplicables a la protección de datos, especialmente la plena vigencia de los derechos de los titulares. El art. 4 de la LOPDP la define indicando: "Autoridad pública independiente encargada de supervisar la aplicación de la presente Ley, reglamento y resoluciones que ella dicte, con el fin de proteger los derechos y libertades fundamentales de las personas naturales, en cuanto al tratamiento de sus datos personales" (LOPDP, 2021).

La independencia de la autoridad de control es un elemento crucial para el cumplimienteo de sus funciones, objetivo que debe perseguirse desde su designación. La doctrina y legislación europea así lo reconocen:

> La importancia de la Independencia de la autoridad de control se ratifica en el RGPD al señalar que el establecimiento en los estados miembros de autoridades de control capacitadas para desempeñar sus funciones y ejercer sus competencias con plena independencia constituye un elemento esencial para la protección de las personas físicas con respecto al tratamiento de datos de carácter personal (Rubí, 2019).

Ecuador decidió crear una superintendencia para que asuma las funciones de autoridad de protección de datos. Consideramos inadecuada tal alternativa de cumplimiento de la norma antes mencionada, al advertir que es el Estado, en todos sus niveles, el que más datos somete a tratamiento y, como consecuencia, con más frecuencia vulnera los derechos y libertades de los ciudadanos. Los superintendentes, según lo establecido en el art. 213 de la CRE, son nombrados según ternas que remite el presidente de la república al Consejo de Participación Ciudadana y Control Social, hecho que compromete su imparcialidad e independencia.

ISSN: 2953 - 6464
DOI: https:/10.53591/dcjcsp.v7i7.2572

El Delegado de Protección de Datos

Este es el último de los elementos subjetivos del sistema de protección de datos. Es una figura nueva en la legislación internacional en protección de datos, pero sus funciones ya existían con anterioridad a su inclusión en el RGPD y, por esa vía en nuestra legislación a partir de la aprobación de la LOPDP en mayo del 2021.

Indica (Rodríguez, 2019) en relación con la aparición normativa de esta figura menciona:

> El origen de la figura del DP o se encuentra en Alemania, que se constituyó en el primer país a nivel internacional en instaurar la figura, y lo hizo en su ley federal de protección de datos personales, conocida como *Beauftragten fur den Datenschutz*. Pese a ello, hay autores que sostienen que el origen del delegado de protección de datos se produjo en el seno de una empresa alemana con anterioridad, incluso, a la precitada normativa
>
> Posteriormente, como consecuencia de una enmienda presentada a la propuesta de DPDP, Expuesta por el parlamento europeo, surgió la figura del DPD, o, como fue conocido por entonces, encargado de la protección de datos, según la traducción española, que hizo que terminara introduciéndose en el texto normativo comunitario.

Las funciones del DPD están orientadas a asesorar al responsable o al encargado del tratamiento de los datos personales en la aplicación de las mejores prácticas para evitar la vulneración de los derechos y libertadas de los titulares de los datos. Se considera parte de las obligaciones que se derivan de la responsabilidad proactiva como obligación del responsable del tratamiento, es decir, en palabras de (Aparicio & Vidal, 2019): "Este principio exige que el responsable del tratamiento tenga que aplicar medidas jurídicas, técnicas y organizativas adecuadas para cumplir y poder demostrar el cumplimiento de la normativa aplicable sobre protección de datos personales". Es por tal motivo que afirmamos que la presencia del DPD, es una señal de la sujeción del responsable del tratamiento de los datos personales al principio de responsabilidad proactiva o *accountability* en el desarrollo de sus actividades.

ISSN: 2953 - 6464
DOI: https:/10.53591/dcjcsp.v7i7.2572

Es evidente que la incorporación de un funcionario con el perfil profesional capaz de orientar a una organización sobre la mejor manera de sujetarse a las normas relacionadas a la protección de datos personales no es fácil de asumir, desde el punto de vista financiaero. Es por tal motivo que no siempre se exige su presencia, ello dependerá de las circunstancias. El considerando 97 del RGPD establece:

> Al supervisar la observancia interna del presente Reglamento, el responsable o el encargado del tratamiento debe contar con la ayuda de una persona con conocimientos especializados del Derecho y la práctica en materia de protección de datos si el tratamiento lo realiza una autoridad pública, a excepción de los tribunales u otras autoridades judiciales independientes en el ejercicio de su función judicial, si el tratamiento lo realiza en el sector privado un responsable cuyas actividades principales consisten en operaciones de tratamiento a gran escala que requieren un seguimiento habitual y sistemático de los interesados, o si las actividades principales del responsable o del encargado consisten en el tratamiento a gran escala de categorías especiales de datos personales y de datos relativos a condenas e infracciones penales. En el sector privado, las actividades principales de un responsable están relacionadas con sus actividades primarias y no están relacionadas con el tratamiento de datos personales como actividades auxiliares. 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. Tales delegados de protección de datos, sean o no empleados del responsable del tratamiento, deben estar en condiciones de desempeñar sus funciones y cometidos de manera independiente (*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)*, s. f.).

ISSN: 2953 - 6464
DOI: https:/10.53591/dcjcsp.v7i7.2572

De acuerdo a la norma comunitaria europea en materia de protección de datos, es mandatoria la presencia de una DPD en los siguients casos: a) Si el tratamiento lo realiza una autoridad pública, a excepción de los tribunales u otras autoridades judiciales independientes en el ejercicio de su función judicial; b) Si el tratamiento lo realiza en el sector privado un responsable cuyas actividades principales consisten en operaciones de tratamiento a gran escala que requieren un seguimiento habitual y sistemático de los interesados; o, c) Si las actividades principales del responsable o del encargado consisten en el tratamiento a gran escala de categorías especiales de datos personales y de datos relativos a condenas e infracciones penales.

Es claro que, en Ecuador, al referirnos a una autoridad pública, nos referimos a aquellas descritas en el art. 225 de la CRE. La salvedad contenida en el considerando 97 del RGPD, no se encuentra en la legislación nacional. El art. 48 de la LOPDP no incluye tal excepción, como consecuencia de lo cual, entendemos que la Función Judicial está también obligada a designar el o los DPD que se requieran para asegurar el correcto tratamiento de los datos personales de las personas involucradas en la administración de justicia.

Se requiere, asímimo, la designación de un DPD, cuando el tratamiento se realice a gran escala. La doctrina europea da algunas pistas, sin definiciones unívocas sobre lo que podriamos reconocer como concepto jurídico indeterminado:

> De hecho, no es posible dar una cifra exacta, ya sea con relación a la cantidad de datos procesados o al número de personas afectadas, que pudiera aplicarse en todas las situaciones. No obstante, esto no excluye la posibilidad de que, con el tiempo, se desarrolle un método estándar para identificar en términos más específicos o cuantitativos qué constituye «a gran escala» con respecto a determinados tipos de actividades de tratamiento comunes. El Grupo de Trabajo del artículo 29 también prevé contribuir a este desarrollo compartiendo y publicando ejemplos de los umbrales pertinentes para la designación de un DPD.

ISSN: 2953 - 6464
DOI: https:/10.53591/dcjcsp.v7i7.2572

> En cualquier caso, el Grupo de Trabajo recomienda que se tengan en cuenta los siguientes factores, en particular, a la hora de determinar si el tratamiento se realiza a gran escala:
>
> - El número de interesados afectados, bien como cifra concreta o como proporción de la población correspondiente;
> - El volumen de datos o la variedad de elementos de datos que son objeto de tratamiento;
> - La duración, o permanencia, de la actividad de tratamiento de datos;
> - El alcance geográfico de la actividad de tratamiento. (*wp243rev01-es.pdf*, s. f.)

Dada la ambigüedad del término, llegado el caso, la autoridad de control en la protección de datos debe establecer, atentas las circunstancias, si un determinado responsable o encargado del tratamiento de los datos personales debe o no contar con el asesoramiento de un DPD, bajo el criterio de tratamiento a gran escala.

En la legislación ecuatoriana, el tratamiento a gran escala debe involucrar categorías especiales, tal como se encuentran definidas en el art. 25 de la LOPDP, es decir, datos relacionados a menores de edad, personas con discapacidad, datos relacionados a la salud y datos sensibles[4].

Otro de los criterios que tornan en obligatoria la presencia en una organización de un DPD, es el seguimiento habitual y sistemático de los interesados. Tampoco en este caso, la legislación nacional o comparada, nos da luces sobre lo que debemos entender por observación habitual o sistemática, recurriremos una vez más a los criterios doctrinarios para entender el alcance del término en cuestion:

> Ejemplos de actividades que pueden constituir una observación habitual y sistemática de interesados son: operar una red de telecomunicaciones; prestar servicios de telecomunicaciones; redireccionar correos electrónicos; actividades de mercadotecnia basadas en datos; elaborar de perfiles y otorgar puntuación con fines

[4] Debemos indicar que la expression datos sensibles, fue cambiada en en RGPD, por datos de categorías especiales. La legislación nacional estructura entre los conceptos, una relación género – especie, mientras que la europea es abarcativa de todas las categorías contenidas en lo que nosotros entrendemos como datos sensibles. A nuesto entender, la distinción que hace nuesrta legislación, es inadecuada.y puede originar confusiones.

ISSN: 2953 - 6464
DOI: https:/10.53591/dcjcsp.v7i7.2572

> de evaluación de riesgos (p. ej. para determinar la calificación crediticia, establecer primas de seguros, prevenir el fraude, detectar blanqueo de dinero); llevar a cabo un seguimiento de la ubicación, por ejemplo, mediante aplicaciones móviles; programas de fidelidad; publicidad comportamental; seguimiento de los datos de bienestar, estado físico y salud mediante dispositivos ponibles; televisión de circuito cerrado; dispositivos conectados, como contadores inteligentes, coches inteligentes, domótica, etc. (*wp243rev01-es.pdf*, s. f.).

De los ejemplos proporcionados por el Grupo de Trabajo del artículo 29 (actual Comité Europeo de Protección de Datos), podemos inferir que observación habitual debe considerarse realizada en un lapso prolongado, o por intervalos que se repiten o realizados mediante una planificación.

El último caso en el que la legislación europea considera mandatoria la presencia de un DPD, es cuando están involucrados datos relativas a condenas o infracciones penales. Tal condición no es considerada en la legislación nacional.

El art. 48.4 de la LOPDP considera un caso para la designación obligatoria de un DPD: "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". Debemos entender el presente caso, relacionándolo con el art. 48.1 *ibidem*, es decir, se trata de información en la que no esté involucrada la seguridad y la defensa nacionales que, por tales, se las considere reservadas o secretas, según lo establecido en el art. 19 de la Ley de Seguridad Pública y del Estado.

Es de extrema importancia indicar que, fuera de los casos en los que es obligatoria la presencia de un DPD en una organización sea esta pública o privada; una organización puede contar con uno, aun cuando no tenga la obligación de hacerlo, pues siempre podrá justificar con su presencia, el cumplimiento de la observancia del principio de responsabilidad proactiva, tal como se expresó en anterioridad.

ISSN: 2953 - 6464
DOI: https:/10.53591/dcjcsp.v7i7.2572

Tratándose del sector privado, la vinculación de un DPD puede ser mediante una relación de dependencia laboral, esto es, mediante un contrato de servicios personales y mediante un contrato de servicios profesionales, en cuyo caso, no existirá obligación laboral alguna con la orgazación contratante. En cuanto al sector público, el reglamento de la LOPDP establece que el DPD deberá ser designado por la máxima autoridad institucional. Entendemos que se trata de la autoridad nominadora del organismo o empresa pública involucrada, por medio de un contrato de servicios ocasiones o nombramiento provisional, mientras se convoca al concurso de méritos y oposición para la vinculación permanente de servidor que desempeñe las funciones de DPD.

Cualquiera sea la figura jurídica empleada para la vinculación del DPD, este cuenta con lo que se podría considerar garantía de estabilidad laboral reforzada, pues se indica en el art. 51:

> […] En caso que el delegado sea sancionado o removido por motivo de la ejecución de sus funciones, podrá poner este hecho en conocimiento de la Autoridad de Protección de Datos Personales, que valorará las circunstancias en las que se produjo la desvinculación o sanción y validará las sanciones que correspondan, sin perjuicio de las acciones legales o judiciales a que hubiere a lugar por parte del delegado perjudicado (*REGLAMENTO DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES*, s. f.)

Si se produjera la cesación del DPD, este podría inciar las acciones legales respectivas, en la medida que justifique que tal cesación se encuentre motivada por alguna decisión que hubiera tomado en el desempeño de sus funciones.

Conclusiones

Como consecuencia del análisis realizado, podemos arribar a las siguientes conclusiones:

El delegado de protección de datos es una figura encaminada a garantizar que el responsable y encargado del tratamiento de los datos personales, se ciña a la finalidad declarada al iniciar

ISSN: 2953 - 6464
DOI: https:/10.53591/dcjcsp.v7i7.2572

el tratamiento y lo hará mediante la supervisión de las actividades de tratamiento y el asesoramiento que corresponda para evitar la afectación de los derechos y libertades de los titulares de los datos personales.

Pese a la *vacatio legis* establecida en la DISPOSICIÓN TRANSITORIA PRIMERA de Ley Orgánica de Protección de Datos Personales, solo después de la designación del superintedente de protección de datos personales, se empezaron a contratar o a designar a los delegados de protección de datos. Tal atraso también provocó la postergación en la formación de profesionales en número suficiente para asumir dichas funciones.

Hasta ahora, la protección de los datos personales no se ha asumido, por parte de la población, ni por aquellos que, como parte de sus actividades comerciales o profesionales, someten a tratamiento los datos personales, como un objetivo que redunda en la vigencia plena de los derechos fundamentales.

Recomendaciones

Para coadyuvar en alcanzar el objetivo del pleno respeto al derecho fundamental a la protección de los datos personales, recomendamos lo siguiente:

La autoridad de protección de datos debe asumir la tarea de difundir agresivamente los derechos de los titulares de los datos personales y las formas de ejercerlos

La autoridad de control de protección de datos debe asumir la formación de profesionales en relación a la protección de datos, mediante cursos coordinador con centro de educación superior, que culminen con la certificación como delegados de protección de datos

Las recientemnte designadas autoridades de control de protección de datos, deben asumirse como generadores de docrtina en protección de datos, tal como lo hace la Agencia Española de Protección de Datos (AEPD), como una contribución a la difusión de la importancia de proteger los datos personales y los graves efectos para los titulares que implica su vulneración.

ISSN: 2953 - 6464
DOI: https:/10.53591/dcjcsp.v7i7.2572

REFERENCIAS BIBLIOGRÁFICAS

Álvarez, J. (2020). *Protección de Datos 2021* (Primera). Aranzadi.

Aparicio, J., & Vidal, M. (2019). *Estudio sobre la protección de datos* (Primera). Aranzadi.

Código Civil, 10 (2005).

Constitución de la República del Ecuador (2008).

Davara, M. (2021). El fichero en la normativa sobre protección de datos personales. El tratamiento total o parcialmente automatizado de datos personales contenidos o destinados a ser incluidos en un fichero (comentarios al art. 2.1 RGPD y al art. 2.1 LOPDGDD. En *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales* (Primera, Vol. 1, p. 330). Thomson Reuters.

Hernández, Ju. C. (2021). Responsable de tratamiento y encargado de tratamiento. En *Tratado de Derecho Digital* (Primera, p. 257). Wolters Kluwer.

Legal, C. (2022, noviembre 28). Encargado de tratamiento o destinatario de datos. *Cumplimiento de la LOPDGDD y el RGPD*. https://coolabora.es/encargado-de-tratamiento-o-destinatario-de-datos/

Ley Orgánica de Protección de Datos Personales, Asamblea Nacional.

Ley Orgánica de Protección de Datos Personales (2021).

Megías, J. (2021). Actividades personales y domésticas excluidas del ámbito de aplicación (comentario al artículo 2.2.C) RGPD y al artículo 2.1.A) LOPDGDD. En *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales: Vol. I* (Primera, p. 355).

¿Qué Son Los Destinatarios? - Legal Box Plus. (2025, marzo 14). https://legalbox.plus/que-son-los-destinatarios-en-proteccion-de-datos/

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

ISSN: 2953 - 6464
DOI: https:/10.53591/dcjcsp.v7i7.2572

y por el que se deroga la Directiva 95/ 46/ CE (Reglamento general de protección de datos). (s. f.).

REGLAMENTO DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES. (s. f.). Recuperado 16 de junio de 2025, de https://app.lexis.com.ec/sistema/visualizador-norma/PUBLICO-REGLAMENTO_DE_LA_LEY_ORGANICA_DE_PROTECCION_DE_DATOS_PERSONALES

Rodríguez, Ju. F. (2019). *Figuras y responsabilidades en el tratamiento de los datos personales* (Primera). Bosch.

Rubí, J. (2019). La Agencia Española de Protección de Datos. En *Tratado de Protección de Datos* (Primera, p. 251). Tirant Lo Blanch.

Wp243rev01-es.pdf. (s. f.). Recuperado 15 de junio de 2025, de https://www.aepd.es/documento/wp243rev01-es.pdf