
Universidad de San Andrés

Departamento de Derecho

Maestría en Derecho Empresario

# Datos personales. Aplicación extraterritorial del reglamento general de protección de datos de la Unión Europea: ¿Cuál es el rol del delegado de protección de datos de empresas argentinas?

Lucía López Laxague
DNI 32.984.927
Director: Santiago Gini
Buenos Aires, 4 de mayo de 2020

ABSTRACT

Este trabajo pretende hacer un análisis del Reglamento General de Protección de Datos de la Unión Europea a fin de entender: (i) en qué supuestos las empresas argentinas deben someterse a sus prescripciones, y (ii) en qué casos esas empresas deberán – además - nombrar un Delegado de Protección de Datos. El trabajo analiza puntualmente la figura del Delegado de Protección de Datos, cada una de las particularidades que surgen de su figura, su rol, funciones, independencia y responsabilidad. Todo ello para llegar a la conclusión de que la designación de un Delegado de Protección de Datos implica un desafío para las empresas que deben nombrarlo. Esto sobre todo teniendo en cuenta el doble rol del Delegado de Protección de Datos que incluye, por un lado, el rol de auditor y por el otro el rol responsable de aplicación de la normativa de protección de datos dentro de esa organización.

## I. INTRODUCCIÓN

El Reglamento General de Protección de Datos de la Unión Europea (*General Data Protection Regulation o* "GDPR" por sus siglas en inglés) implicó una reforma importante en la regulación que la Unión Europea tenía sobre datos personales. El GDPR fue aprobado por el Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo del 27 de abril de 2016 y que entró en vigencia para todos los países miembros de la Unión Europea el 25 de mayo de 2018[1].

El ámbito de aplicación del GDPR incluye no sólo a las empresas ubicadas en territorio europeo sino también para muchas empresas que, sin estar localizadas en la Unión Europea, tienen algún tipo de conexión, en los términos del propio GDPR, con ese territorio[2]. Dado que estos tipos de conexión del GDPR son bastante amplios, gran cantidad de empresas argentinas deben o deberán en algún momento, aplicar el GDPR[3].

Una de las novedades introducidas por el GDPR es la figura del delegado de protección de datos (*Data Protection Officer* o "DPO" por sus siglas en inglés). El DPO es una persona nombrada por cada responsable o procesador de datos o bases de datos y tiene a su cargo la obligación de velar para que tal responsable o procesador cumpla con los estándares de protección de datos establecidos por el GDPR.

---

1 GDPR - Reglamento General de Protección de Datos de la Unión Europea. s.f. «EUR-Lex.» Disponible el 06 de marzo de 2020 en https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A32016R0679

2 Analizaré más abajo a lo largo de este trabajo en qué el GDPR establece que hay una conexión con el territorio de la Unión Europea.

3 A continuación, detallo algunas notas periodísticas que hacen referencia al hecho de que empresas argentinas han empezado a implementar la normativa del GDPR: https://www.abogados.com.ar/argentina-se-adapta-a-la-normativa-europea-mientras-espera-la-sancion-de-la-nueva-ley-de-proteccion-de-datos-personales/22921; https://tn.com.ar/tecno/f5/reglamento-general-de-proteccion-de-datos-europeo-como-afecta-en-argentina_871256; https://es.ccm.net/faq/31402-que-es-el-reglamento-general-de-proteccion-de-datos-rgpd-de-la-union-europea; o https://www.iproup.com/innovacion/7532-hacker-innovacion-social-inventos-tecnologicos-Seguridad-datos-Internet-que-es-el-compliance

El propósito general de este trabajo consiste en: (i) explicar en qué medida el GDPR es aplicable a las empresas argentinas; y (ii) analizar la figura del DPO con el objeto de entender qué responsabilidades y deberes le caben a los DPO designados por empresas argentinas y cuál es el alcance de su responsabilidad.

En la primera parte del trabajo, haré una breve descripción del GDPR para luego centrarme en dos aspectos específicos. Por un lado, el alcance extraterritorial de la norma a fin de entender en qué medida el GDPR es aplicable a empresas argentinas, y por el otro lado, el concepto de responsabilidad activa o *accountability*.

El principio de responsabilidad activa rige todo el GDPR y, tal como explicaré más adelante, pone en cabeza del responsable o procesador de datos la tarea de determinar qué estándares de protección de datos aplicará en función de las características personales de su empresa y del tipo de datos que procesa. Este principio de responsabilidad es aplicable también a las características personales que deberá tener el DPO designado en cada caso particular como así también al tipo de tareas que deberá desarrollar y al alcance de sus responsabilidades.

En la segunda parte del trabajo analizaré la figura del DPO. Para ello, empezaré por hacer una comparación con otras figuras similares, describiendo los antecedentes normativos del DPO y la existencia de figuras similares en el ordenamiento argentino. Luego, intentaré definir en qué casos una empresa está obligada por el GDPR a nombrar un DPO para lo que analizaré cada uno de los supuestos establecidos en el GDPR, incluyendo el concepto de análisis masivo de datos y de grupo económico.

Finalmente, describiré el tipo de tareas a cargo del DPO, la característica de su trabajo y el concepto de independencia y confidencialidad. Todo ello con el objeto de entender cuáles son las obligaciones de los DPO nombrados por empresas argentinas y el alcance de su responsabilidad bajo el GDPR.

## II. LA NORMATIVA DE PROTECCIÓN DE DATOS

La normativa sobre protección de datos varía según cada país o jurisdicción. Sin embargo, y con independencia del nivel de exigencia de cada una de las normas particulares sobre la materia, todas buscan proteger los derechos de los titulares de los datos a fin de resguardar su derecho a la libertad, la intimidad, al honor y/o la privacidad, entre otros.

Los reguladores de los distintos países han dictado estas normas de la protección de datos en un contexto donde la globalización facilita las operaciones transfronterizas y la tecnología permite procesar cantidades masivas de datos e internet permite su divulgación instantánea. Todas estas realidades y herramientas bien utilizadas mejoran la calidad de vida de muchas personas.

Sin embargo, potencian también las filtraciones y el uso indebido de los datos personales pudiendo afectar la libertad, la intimidad, el honor y la privacidad de las personas. Es por ello que han aparecido, en la mayoría de las jurisdicciones, normativas que buscan proteger los datos personales de las personas.

Resulta difícil por otro lado, tal como sostiene PALAZZI[4], encontrar en los modelos de negocios actuales alguna empresa que no requiera el manejo de cierta clase de datos para

[4] Palazzi, Pablo A. *Compliance y protección de datos personales* Publicado en: Sup. Esp. Compliance 2018 (mayo), 18/05/2018, 405

poder desarrollar sus actividades. Esto implica que casi todas las empresas del mundo de hoy deban cumplir con el derecho aplicable sobre protección de datos.

PALAZZI[5] explica que cada normativa de datos define ciertos estándares de protección que deben cumplir aquellas personas que procesan o almacenan datos personales. Dentro de estos estándares de protección, además de las medidas de seguridad que deba tomar quién sea responsable de la base de datos, se suelen establecer limitaciones respecto del tiempo y la finalidad para la que se recaban los datos y de la forma en que esos datos pueden transferirse a terceros dentro y fuera de una jurisdicción.

Las normativas sobre protección de datos también establecen derechos a los titulares de los datos. Para ello, regulan los mecanismos necesarios para que cada titular pueda solicitar la modificación, rectificación y/o supresión de sus datos de una determinada base de datos[6].

Finalmente, se suelen crear también procesos administrativos o judiciales para hacer cumplir esos derechos. Tal es el caso, por ejemplo, de la acción *habeas data* contemplada en nuestro ordenamiento jurídico.

## III. EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

En este apartado haré una descripción general del GDPR para luego revisar puntualmente tres aspectos que considero fundamentales a los efectos de este trabajo: (i) el principio de aplicación extraterritorial del GDPR; (ii) el principio de responsabilidad proactiva y (iii)

[5] Palazzi, Pablo A. *Compliance y protección de datos personales* Publicado en: Sup. Esp. Compliance 2018 (mayo), 18/05/2018, 405

6 En algunos cuerpos normativos como el GDPR se prevé también el derecho al olvido como un derecho de los titulares de los datos.

los efectos del GDPR sobre empresas argentinas.

### A. Descripción general

Como escribí al principio de este documento, el 25 de mayo de 2018 entró en vigencia el GDPR que es catalogado por autores como FRENE como el nuevo estándar mundial en temas de protección de datos[7]. Esto no solo por los altos estándares para la protección de datos personales que contiene sino también por sus efectos extraterritoriales.

Lo primero que debe indicarse es que el GDPR es una norma de aplicación vinculante para todos los países que conforman la Unión Europea por lo que, bajo el derecho de la Unión Europea, no requiere de la sanción de normas internas que lo reglamenten o que determinen su aplicación[8]. En este sentido, el GDPR es aplicable, con independencia de la legislación local que cada uno de los países miembros de la Unión Europea haya sancionado en relación a la protección de datos personales.



El considerando 6 del GDPR establece: "*la rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales. La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades. Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial. La tecnología ha transformado tanto la*

[7] Frene, Lisandro, *Reglamento general de protección de datos de la unión europea. Extraterritorialidad e impacto en argentina*. 2018. La Ley (LA LEY 2018-E, 1275 - Cita Online: AR/DOC/1764/2018).

[8] A diferencia por ejemplo de las directivas que en actos legislativos en los cuales se establecen objetivos que todos los países de la Unión Europea deben cumplir, correspondiendo a cada país elaborar sus propias leyes sobre cómo alcanzar esos objetivos (para más información ver https://europa.eu/european-union/eu-law/legal-acts_es).

*economía como la vida social, y ha de facilitar aún más la libre circulación de datos personales dentro de la Unión y la transferencia a terceros países y organizaciones*".

En efecto, la integración económica y social entre los países de la Unión Europea aumentó considerablemente el flujo transfronterizo de datos personales. Este hecho, entre otros, motivó la sanción de una norma como el GDPR.

El principal objetivo de la sanción del GDPR es el de proteger el derecho a la protección de datos de las personas, así como también "*contribuir a la plena realización de un espacio de libertad, seguridad y justicia y de una unión económica, al progreso económico y social, al refuerzo y la convergencia de las economías dentro del mercado interior, así como al bienestar de las personas físicas*"[9]. El GDPR tiene además entre sus objetivos garantizar la libre circulación de los datos personales a través de la Unión Europea mediante un estándar normativo similar para todos los países que integran la Unión Europea[10].



Con anterioridad a su sanción, las legislaciones de cada uno de los países que conforman la Unión Europea, contenían distintos niveles y regulaciones sobre protección de datos. Esta situación generaba cierto *forum shopping* entre los distintos responsables de tratamiento de datos, que buscaban radicarse en aquellas jurisdicciones que tuvieran una normativa más flexible por lo que la sanción del GDPR tuvo también por objeto garantizar que, dentro de la Unión Europea, las normas de protección de datos sean coherentes y homogéneas.

[9] Considerando 2 del GDPR
[10] Considerando 5 del GDPR

En relación al ámbito de aplicación del GDPR se deben destacar dos aspectos importantes. Por un lado, en relación al ámbito de aplicación material se limitó la aplicación del GDPR los datos personales de personas humanas y no de personas de existencia ideal dado que el GDPR busca principalmente garantizar los derechos y libertades fundamentales de los habitantes de la Unión Europea.

Por otro lado, y en relación al ámbito de aplicación territorial, el GDPR fue aún más lejos porque estableció su aplicación para responsables y procesadores de tratamiento de datos que se encuentren fuera de la Unión Europea en una gran cantidad de casos. Me dedicaré a este aspecto en el próximo apartado.

**B. Aplicación extraterritorial del GDPR**

En lo que respecta al objeto de este trabajo, es fundamental entender en qué casos y en qué medida, el GDPR resulta aplicable fuera de las fronteras de la Unión Europea. Esto para poder definir cuándo una empresa argentina está obligada a aplicarlo y en qué casos está también obligada a nombrar un DPO.

Para limitar el ámbito de aplicación, empezaré por lo más siempre y es enumerar los casos en que el GDPR no es aplicable. Según la propia norma, el GDPR no se aplica al tratamiento de datos personales (i) fuera del ámbito de aplicación del derecho de la Unión Europea; (ii) por parte de los estados miembros de la Unión Europea cuando lleven a cabo actividades relacionadas con la política exterior y la seguridad común[11]; (iii) llevado a cabo por personas humanas en el marco de sus actividades personales o domésticas; y

[11] Actividades comprendidas en el ámbito de aplicación del capítulo 2 del título V del Tratado de la Unión Europea.

(iv) por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención[12].

La primera excepción que enumeré en el párrafo anterior lleva a preguntarse en qué casos el tratamiento de datos personales entra dentro del ámbito de aplicación del derecho de la Unión Europea. Nos encontramos aquí frente a una de las cuestiones más controvertidas del GDPR y es la de su aplicación extraterritorial.

Previo a la sanción del GDPR, la normativa europea sobre protección de datos tenía criterios de aplicación esencialmente territoriales por lo que la normativa se aplicaba a aquellos establecimientos ubicados dentro de la Unión Europea. Sin embargo, en el mundo digital en el que vivimos que permite la transferencia de datos a través de las fronteras de un país con un solo *click*, generó la necesidad de cambiar este paradigma respecto de la forma de aplicación de las normas sobre protección de datos.



Tal como adelanté, uno de los aspectos más relevantes y controvertidos de las reformas a la normativa de protección de datos introducidas por el GDPR es el cambio de óptica para determinar en qué situaciones corresponde aplicar el GDPR. Así, se dejó de lado una perspectiva territorial para pasar a una perspectiva basada en el destino del tratamiento que se hace de los datos.

El nuevo enfoque deja de lado la ubicación física de los responsables o encargados de tratamiento de datos para tomar como criterio el destino que se le dará a los datos que se

[12] Artículo 2 del GDPR.

procesen. Este nuevo enfoque convierte sino a todas las empresas del mundo, a una gran cantidad de ellas en potenciales sujetos obligados para el GDPR.

En el enfoque del destino yo no importa si el responsable o procesador de los datos se encuentra ubicado dentro del territorio de la Unión Europea, sino que lo importa es el destino para el que se tratan los datos. Si el destino tiene algún tipo de impacto dentro de la Unión Europea se aplicará el GDPR.

Para entender cuándo un tratamiento tiene algún tipo de impacto en la Unión Europea, se deberá, en primer lugar, analizar puntos de conexión entre el derecho de la Unión Europea y el destino del tratamiento de los datos. Cuanto mayores sean los puntos de conexión, mayor será la certeza respecto de la aplicación del GDPR.

El artículo 3 del GDPR establece el ámbito de aplicación del GDPR y enumera cuales son esos puntos de conexión a tener en cuenta. Lo transcribo a continuación para poder analizar cada uno de los supuestos a continuación:

> "*1. El presente Reglamento se aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no.*
>
> *2. El presente Reglamento se aplica al tratamiento de datos personales de interesados que residan*[13] *en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con: a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o b) el control de su comportamiento, en la medida en que este tenga lugar en la Unión.*

[13] En la versión en inglés del GDPR habla de interesados que "estén" en la Unión Europea. Esto seguramente será objeto de interpretación en un futuro.

*3.El presente Reglamento se aplica al tratamiento de datos personales por parte de un responsable que no esté establecido en la Unión sino en un lugar en que el Derecho de los Estados miembros sea de aplicación en virtud del Derecho internacional público*"[14].

Analizaré por separado cada uno de los supuestos del artículo 3 del GDPR. Este análisis permitirá entender en qué casos las empresas argentinas quedarían comprendidas dentro del ámbito de aplicación del GDPR.

El inciso 1 establece "1. *El presente Reglamento se aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no"*. Este inciso aplica el criterio de territorialidad que ya estaba contemplado en la normativa anterior sobre datos personales bajo el cual todos los responsables o encargados que tengan su establecimiento en la Unión, tendrán que aplicar el GDPR.

Se agrega sin embargo la última parte del inciso "*independientemente de que el tratamiento tenga lugar en la Unión o no".* Este agregado fue especialmente incorporado para justificar la aplicación del GDPR en aquellos casos donde el procesamiento de los datos se hacía fuera de la Unión Europea, ya sea para abaratar costos o bien para evitar la aplicación de la normativa europea en materia de protección de datos.

[14] El GDPR define como *establecimiento* al lugar donde se encuentra la administración central de un responsable o encargado de datos. Se entiende por *responsable* a la persona que determina los fines y medios para el tratamiento de ciertos datos y por *encargado* a la persona que trate los datos por cuenta y orden del responsable. Finalmente, se entiende por *tratamiento* cualquier operación realizada sobre datos personales, ya sea por procedimientos automatizados o no. Son ejemplos de tratamiento de datos la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

Se trata esencialmente de aquellos casos en que, un responsable o encargado establecido dentro de la Unión Europea, contrata el servicio de tratamiento o almacenamiento de datos a una empresa localizada fuera de la Unión Europea. En estos casos, el GDPR será de aplicación no solo a la empresa establecida dentro de la Unión Europea sino también a aquellas empresas a quienes se les haya encomendado el tratamiento o almacenamiento de esos datos.

La norma tiene sentido si se la estudia a la luz del concepto de transferencia internacional de datos. En este marco, si el dato fue recabado de su titular bajo un derecho de la Unión Europea, es lógico que se pretenda mantener el mismo estándar de protección aun cuando el dato sea tratado o almacenado fuera del territorio de la Unión Europea.

Un ejemplo de empresa argentina que deba aplicar el GDPR bajo este punto 3.1. del GDPR sería aquella contratada por una empresa localizada dentro de la Unión Europea para procesar datos relativos a búsquedas laborales a través de un *software* específico. En ese caso tal empresa argentina, deberá cumplir con el régimen del GDPR.

Analizaremos ahora el inciso 2 del artículo 3 del GDPR que crea el enfoque del destino de los datos a que hacía referencia más arriba: "2. *El presente Reglamento se aplica al tratamiento de datos personales de interesados que residan*[15] *en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con: a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o b) el*

15 En la versión en inglés del GDPR habla de interesados que "estén" en la Unión Europea. Esto seguramente será objeto de interpretación en un futuro.

*control de su comportamiento, en la medida en que este tenga lugar en la Unión".*

Este inciso 2 establece en qué casos será de aplicación el GDPR para aquellos responsables o encargados de datos que no estén establecidos dentro de la Unión Europea. Los considerandos del propio GDPR establecen que para determinar si una empresa ofrece bienes o servicios a personas interesadas que residan en la Unión, debe estudiarse si es evidente que el responsable o el encargado proyecta ofrecer servicios a interesados en uno o varios de los estados miembros de la Unión Europea.

En este marco, el considerando 23 del GDPR también establece que "*si bien la mera accesibilidad del sitio web del responsable o encargado o de un intermediario en la Unión, de una dirección de correo electrónico u otros datos de contacto, o el uso de una lengua generalmente utilizada en el tercer país donde resida el responsable del tratamiento, no basta para determinar dicha intención, hay factores, como el uso de una lengua o una moneda utilizada generalmente en uno o varios Estados miembros con la posibilidad de encargar bienes y servicios en esa otra lengua, o la mención de clientes o usuarios que residen en la Unión, que pueden revelar que el responsable del tratamiento proyecta ofrecer bienes o servicios a interesados en la Unión*"[16].

Por su parte, en relación al comportamiento establecido en el artículo 3.2.b., el considerando 24 del GDPR establece que "*para determinar si se puede considerar que una actividad de tratamiento controla el comportamiento de los interesados, debe evaluarse si las personas físicas son objeto de un seguimiento en internet, inclusive el potencial uso posterior de técnicas de tratamiento de datos personales que consistan en*

[16] Considerando 23 GDPR.

*la elaboración de un perfil de una persona física con el fin, en particular, de adoptar decisiones sobre él o de analizar o predecir sus preferencias personales, comportamientos y actitudes*". Este artículo fue pensado especialmente para los proveedores de cuentas de e-mail y redes sociales que monitorean el comportamiento de las personas con distintos fines, entre ellos publicitarios.

Respecto del inciso 3.2.a. - *la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago* - ciertos autores entienden que, si el único punto de conexión entre un procesador de datos y la Unión Europea es el hecho de que el titular de los datos es residente de la Unión, no es de aplicación el artículo 3.2. del GDPR[17]. Siguiendo este razonamiento, si un turista italiano comprara un mate de recuerdo en algún local de la calle Florida en Buenos Aires, no podría entenderse que, por esa sola razón, el local de la calle Florida tenga que aplicar el GDPR.

Sin embargo, la situación es distinta si se trata de una empresa que vende sus productos por internet al mundo entero y no en especial a la Unión Europea - por ejemplo, una empresa que desarrolla algún insumo de agro. En este caso, esa empresa no está ofreciendo sus productos solamente a la Unión Europea, sino también a Estados Unidos, Australia, o cualquier otro país donde pueda venderse.

En ese caso, es probable que la página web no esté solo en español, sino también en

[17] Paul de Hert, Michal Czerniawski; *Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context*. International Data Privacy Law, Volume 6, Issue 3, 1 August 2016, Pages 230–243, Disponible el 03.03.2020 en https://doi.org/10.1093/idpl/ipw008.

inglés. No queda aquí del todo claro si los puntos de conexión son suficientes como para que la empresa tenga que aplicar o no el GDPR.

Llegado el caso de que un residente de la Unión Europea decida adquirir alguno de esos productos, pareciera que la empresa argentina debiera aplicar el GDPR. Sin embargo, si la mayoría de los clientes extranjeros de esa empresa no residen en la Unión Europea y la compra de un producto es una situación aislada, habría argumentos para defender la postura de que, esa empresa, no debe aplicar el GDPR.

El GDPR intenta de alguna manera limitar los casos en que resulta aplicable agregando los vocablos *"la oferta de bienes o servicios a dichos interesados en la Unión"* pero la incertidumbre sigue siendo grande dado que no siempre es tan simple determinar si la oferta de bienes o servicios fue efectivamente hecha a personas dentro de la Unión, en especial cuando se trata de empresas que ofrecen sus bienes o servicios por internet. Será entonces cuestión de analizar en cada caso en particular la cantidad de puntos de conexión que existan con la Unión Europea para definir si es aplicable o no el GDPR.

Finalmente, en el caso del punto 3.2.b. se establece que el control del comportamiento que se pretende revisar *"tenga lugar en la Unión"*[18]. En este caso el punto de conexión es más claro porque los comportamientos o actitudes que se monitoreen deben ocurrir dentro de la Unión Europea por lo que queda claro que, en la medida en que ocurran allí, la empresa que esté llevando a cabo deberá aplicar el GDPR.

El artículo 3.2. es uno de los puntos que más controversias ha generado entre los autores.

[18] El subrayado es mío.

Como ya escribí más arriba, su redacción es tan amplia que deja vacíos legales respecto de muchas situaciones, sobre todo aquellas que tienen que ver con la oferta de bienes y servicios a través de internet.

Sin ánimos de entrar en esa discusión que no es el objeto de este trabajo, es importante destacar que, la falta de claridad respecto de qué puntos de conexión se requieren para considerar que en una situación se aplique el GDPR, podría vulnerar el ejercicio de ciertos derechos básicos como el derecho de legalidad, de juez natural y debido proceso o de no ser juzgado dos veces por el mismo tema. Esto en la medida en que sea potencialmente aplicable el GDPR, además de la ley del país donde la empresa esté ubicada.

A modo de conclusión preliminar, entonces, el GDPR será de aplicación para las empresas argentinas que: (i) de alguna manera procesen, traten o almacenen datos de residentes de la Unión Europea por cuenta y orden de un responsable o encargado de tratamiento que tenga su establecimiento en la Unión, (ii) cuando trate datos personales con el objeto de monitorear conductas o comportamiento de personas dentro de la Unión Europea, y (iii) cuando ofrezca bienes y servicios dentro de la Unión. En este último caso, teniendo en cuenta el hecho de que la venta de bienes y servicios a través de internet potencia enormemente las posibilidades de que resulte de aplicación el GDPR aun cuando el mercado principal que se intente captar no sea de la Unión Europea.

**C. Responsabilidad proactiva**

El GDPR se rige por un principio fundamental para los responsables de tratamiento de datos personales que se conoce como el principio de responsabilidad proactiva o *accountability*. Este principio aparece en Argentina en algunas normas tales como la ley

de responsabilidad penal empresaria o en alguna normativa de la Unidad de Información Financiera sobre prevención de lavado de activos y financiación del terrorismo.

El principio de responsabilidad activa exige por parte de las empresas responsables de tratamientos de datos una actitud consciente, diligente y proactiva para cumplir con el GDPR. El principio pone en cabeza de las empresas responsables de tratamiento de datos, la obligación de determinar qué medidas de protección de datos aplicarán a fin de minimizar lo máximo posible cualquier daño a los titulares de los datos y garantizar así el cumplimiento del GDPR.

Para ello, deben realizar una auditoría interna que les permita evaluar cuales son las medidas que deberán aplicar. Para hacer esa auditoría, deberá tenerse en cuenta, entre otros factores: la actividad que realiza la empresa y su tamaño, el tipo de datos que procesa, la tecnología utilizada, los lugares donde opera, la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como el riesgo para los derechos y libertades de las personas y en general cualquier otra información relevante.

Sobre este punto es importante destacar que la auditoría interna permitirá generar una matriz de riesgo que deberá mantenerse actualizada en forma constante. En función del principio de proporcionalidad, las medidas que se tomen para proteger los datos personales, deberán guardar proporción con la matriz de riesgo que se haya preparado.

Así, cuanto mayor sea el riesgo para los derechos de los titulares de los datos, mayores deberán ser las medidas precautorias que el responsable de tratamiento deba tomar. Por el contrario, y en función del principio de proporcionalidad, cuando menor sea el riesgo,

menores las medidas precautorias que deberán tomarse.

En este sentido, el considerando 76 del GDPR establece que "*la probabilidad y la gravedad del riesgo para los derechos y libertades del interesado debe determinarse con referencia a la naturaleza, el alcance, el contexto y los fines del tratamiento de datos. El riesgo debe ponderarse sobre la base de una evaluación objetiva mediante la cual se determine si las operaciones de tratamiento de datos suponen un riesgo o si el riesgo es alto*".

En consecuencia, el tipo de medidas que se tomarán para cumplir con el GDPR dependerá de cada empresa y del resultado de su auditoría de riesgo: algunas medidas serán especialmente útiles para empresas que procesan datos sensibles mientras que tales medidas no serán necesarias para empresas que no procesan ese tipo de datos. Tampoco serán iguales las medidas que deba aplicar una empresa con magnitudes multinacionales en comparación con aquellas medidas que debiera aplicar una empresa pequeña con pocos empleados y un ámbito de aplicación esencialmente local.

El principio de responsabilidad proactiva o *accountability*, exige a las empresas no solo establecer las medidas necesarias que, en función de cada tipo de empresa, permitan el cabal cumplimiento del GDPR sino también poder demostrar que han tomado todas las medidas necesarias para cumplir con esas obligaciones[19]. Para ello, el artículo 30 del GDPR establece que la empresa debe contar con pruebas y documentación suficiente que pruebe el análisis de riesgo realizado y la consecuente implementación de las medidas

[19] Thibaut D'hulst and Lily Kengen "*Data protection compliance strategy".* Van Bael & Bellis

que correspondan[20].

En resumen, el principio de responsabilidad proactiva exige que cada empresa: (i) haga un estudio de riesgo en función de sus características particulares; (ii) establezca las medidas de protección de datos a implementar para cumplir con el GDPR; (iii) determine las responsabilidades de cada agente y área; (iv) establezca medidas de actualización permanente de los riesgos y medidas a tomar en consecuencia; y (v) documente todo el proceso para poder demostrarlo.

**D. Efectos sobre las empresas argentinas**

Como bien se puede observar del análisis del GDPR que hicimos hasta ahora, el GDPR es aplicable a gran cantidad de empresas argentinas. Otras empresas todavía no deben aplicarlo, pero es posible que deban hacerlo en algún momento si realizan alguna de las actividades establecidas en el artículo 3 del GDPR.



No existen todavía sanciones a empresas radicadas fuera de la Unión Europea. Sin embargo se especula con distintas sanciones comerciales como por ejemplo, el bloqueo de los sitios de internet para la Unión Europea[21].

Por su parte, el GDPR prevé por incumplimiento de alguna de sus normas multas administrativas de entre diez y veinte millones de euros hasta entre el 2% o 4% del volumen del negocio global anual de una empresa (lo que sea mayor), dependiendo del

[20] Palazzi, Pablo A. "Compliance y protección de datos personales". Sup. Esp. Compliance 2018 (mayo), 18/05/2018, 405

[21] Frene, Lisandro, *Reglamento general de protección de datos de la unión europea. Extraterritorialidad e impacto en argentina*. 2018. La Ley (LA LEY 2018-E, 1275 - Cita Online: AR/DOC/1764/2018)

tipo de infracción. El GDPR prevé la posibilidad de que los estados miembros impongan otro tipo de sanciones.

Como podrá apreciarse, las sanciones son tan fuertes que es recomendable que cada una de las empresas argentinas que tengan algún punto de conexión con Europa, analicen si corresponde o no que apliquen el GDPR. Esto por supuesto, con independencia de la vocación a tratar los datos personales a cargo de cada empresa de acuerdo con la legislación aplicables y, fundamentalmente, con los mayores estándares de protección que puedan asumirse en cada circunstancia.

En este trabajo nos limitaremos solamente a uno de los tantos aspectos del GDPR que las empresas argentinas que resulten sujetos obligados deben cumplir y es del DPO. Analizaremos a continuación su figura, en qué casos debe ser designado y cuáles son sus obligaciones y responsabilidades.



## IV. EL DELEGADO DE PROTECCIÓN DE DATOS

Analizaré en este apartado el concepto de DPO para lo que, en primer lugar, haré una breve referencia al nacimiento de esta figura y su comparación con otras figuras similares en el derecho argentino. Luego, en segundo lugar, delimitaré, dentro del gran universo de empresas que deben cumplir con el GDPR, cuáles de ellas deben también nombrar un DPO.

En tercer lugar, y ya relacionado directamente con la figura del DPO, analizaré las cualidades personales que debe revestir una persona u organización para poder actuar como DPO. En cuarto lugar, haré una referencia al rol del DPO dentro de una

organización haciendo especial hincapié en los conceptos de independencia, confidencialidad y conflicto de interés. Finalmente, analizaré la responsabilidad del DPO según lo establecido en el GDPR y en otras normativas nacionales.

### A. Concepto y comparación con otras figuras similares

Las "*Directrices sobre los delegados de protección de datos (DPD)*" (las "Directrices")[22] definen al DPO como el elemento central para el cumplimiento de las disposiciones del GDPR. El DPO creado por GDPR es una especie de agente de auditoría o *compliance* que tiene a su cargo velar por el cumplimiento del GDPR por parte de la organización a la que pertenece.

Algunos autores como ROSS, entienden que el DPO es sobre todo eso, un agente de *compliance*[23]. Sin embargo, sus tareas y responsabilidades son tantas que, desde mi punto de vista, se trata de un puesto mucho más amplio que solamente el de auditar el cumplimiento de un sistema de normas.



[22] El Grupo de trabajo sobre protección de datos del artículo 29 (GT 29) fue creado por la Directiva 95/46/EC como órgano consultivo independiente en temas de protección de datos. El GDPR reemplazó la Directiva 95/46/EC y creó un nuevo órgano consultivo independiente denominado Comité Europeo de Protección de Datos que reemplazó al GT 29. Sin embargo, una vez aprobado el GDPR y antes de que entre en vigencia, el GT 29 dictó una serie de guías y directrices relacionadas con la aplicación del futuro GDPR. El Comité Europeo de Protección de Datos, mediante resolución 1/2018 recomendó varias de las guías y directrices que en su momento había sancionado el GT 29. Entre ellas, el Comité Europeo de Protección de Datos aprobó específicamente las "*Directrices sobre los delegados de protección de datos (DPD)*" (WP 243 rev.01. Adoptadas el 13 de diciembre de 2016 y revisadas por última vez y adoptadas el 5 de abril de 2017. Estas Directrices estaban disponibles el 22 de febrero de 2020 en https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf). Por el momento el Comité Europeo de Protección de Datos no ha hecho modificaciones o revisiones a estas Directrices sobre DPO y tampoco ha emitido nuevas recomendaciones sobre este tema puntual. Las citaré en muchas oportunidades a lo largo de este trabajo en tanto comprenden una interpretación de un organismo de la Unión Europea sobre el objeto de este trabajo.

[23] Ross, David "GDPR and the Role of the Data Protection Officer". Octubre 1, 2018. Disponible el 2 de febrero de 2020 http://www.rmmagazine.com/2018/10/01/gdpr-and-the-role-of-the-data-protection-officer

En este marco un DPO, además de sus funciones de auditoría, tiene a su cargo la implementación dentro de su organización de todas las políticas relativas a la protección de datos. Y es, finalmente y no por eso menos importante, el responsable de la creación y desarrollo de una cultura organizacional a luz de la normativa de protección de datos.

Estas últimas funciones son, desde mi perspectiva, la más importantes. Al respecto, las Directrices establecen que "*es importante que el [DPO] sea considerado como un interlocutor dentro de la organización y que forme parte de los correspondientes grupos de trabajo que se ocupan de las actividades de tratamiento de datos dentro de la organización*"[24].

Vale destacar por otro lado que la figura del DPO no es nueva. La novedad es que, a partir de la sanción del GDPR, cierta categoría de organizaciones que detallaré más abajo, tendrán la obligación de nombrar uno.

Figuras similares al DPO, sobre todo desde el punto de vista de su función de auditor, ya existían en algunos países no solo para temas de protección de datos sino, por ejemplo, para cuestiones relativas al lavado de activos y financiación del terrorismo. Legislaciones nacionales sobretodo europeas y anteriores al GDPR, habían creado –además- algún tipo de figura similar para temas de protección de datos.

Así, siguiendo la explicación de RECIO[25], en Alemania la figura del DPO apareció por primera vez en 1977 en la *Bundesdatenschutzgesetz*, la ley de protección de datos

[24] Punto 3.1. de las Directrices.
[25] Recio, Miguel. "Data Protection Officer: The Key Figure to Ensure Data Protection and Accountability", 3 Eur. Data Prot. L. Rev. 114 (2017) Disponible el 10 de diciembre de 2018 en HeinOnline.

alemana. Francia por su parte también había incorporado una figura similar denominada "*correspondant a la protection des donndes*".

En el derecho argentino, la figura del DPO se asemeja en cierto sentido al oficial de cumplimiento creado por la ley 25.246[26]. El oficial de cumplimiento es, bajo esta normativa, responsable de velar por la observancia e implementación de los procedimientos y obligaciones para la prevención del lavado de activos y el financiamiento del terrorismo y de formalizar las presentaciones ante la Unidad de Información Financiera.

Sin embargo, la figura de oficial de cumplimiento no es igual a la del DPO. Tal como remarqué anteriormente, entiendo que la figura del DPO es más amplia y tiene a su cargo muchos más aspectos operativos que el oficial de cumplimiento, en lo que respecta puntualmente a la protección de datos personales.



**B. Sujetos que deben nombrar un DPO**

El GDPR establece que cierta categoría de responsables o encargados de tratamiento deben nombrar un DPO. La falta de cumplimiento de esta obligación puede acarrear sanciones para aquellos responsables o encargados que no la cumplan.

Las sanciones pueden consistir en multas administrativas de hasta diez millones de euros o el equivalente al 2% del volumen de negocio total anual global del ejercicio financiero

[26] La Ley 25.249 que crea ciertos tipos penales para delitos relacionados con el encubrimiento y lavado de activos de origen delictivo, es la primera ley argentina que establece algún tipo de obligación de *compliance*. Esta ley es la norma que da lugar a la infinidad de resoluciones de la Unidad de Información Financiera para las distintas entidades que son sujetos obligados en los términos de la ley. Entre otras cosas, esta ley establece la obligación por parte de las empresas de implementar una política de conocimiento del cliente y la obligación de nombrar un oficial de cumplimiento.

anterior[27]. Por otro lado, si la sanción ocurriera por otro tipo de incumplimiento distinto al incumplimiento de las disposiciones relativas al DPO, la designación o no de un DPO y el rol que haya ejercido podrían servir también como atenuante o agravante a la hora de aplicar una sanción.

Existe también una segunda categoría de empresas que por el tipo de actividad que realizan no tienen obligación bajo el GDPR de nombrar un DPO. Sin embargo, a la luz del principio de responsabilidad proactiva, pueden llegar a tomar la decisión de nombrar uno.

Finalmente, existe una tercera categoría de empresas. Esta categoría incluye aquellas empresas que, sin estar encuadradas en la categoría de empresas obligadas a nombrar un DPO, deciden nombrar algún tipo de responsable de datos personales, pero sin que esa persona sea un DPO en los términos del GDPR.



En este apartado, me ocuparé sobretodo de los casos en que el nombramiento de un DPO es obligatorio. Sin embargo, dedicaré un apartado especial a la segunda y tercera categoría de empresas, es decir aquellas que deciden nombrar un DPO voluntario o las que, dentro de su estructura, tienen un agente responsable de datos personales.

i. DPO obligatorio

El GDPR establece en qué casos, los responsables o encargados de datos deberán nombrar un DPO. Esta obligación aplica tanto responsables como a encargados de datos. A partir

[27] Conforme al artículo 83 del GDPR. En la versión en inglés la frase "volumen del negocio total anual global del ejercicio financiero" está definida como "*total worldwide annual turnover of the preceding financial year*". Si bien la definición no es del todo clara y queda sujeta a interpretación, podrían entenderse como que se trata del volumen de facturación o ingresos.

de ahora no haré una distinción específica para responsables o encargados de tratamiento, sino que en general me referiré a ellos como la "organización" o la "empresa" en forma indistinta.

Sin perjuicio de lo anterior, es importante destacar que, en algunas ocasiones ambos actores – el responsable de datos y el encargado de tratamiento - deberán nombrar un DPO. Sin embargo, no siempre será así.

A veces un responsable de datos puede tener obligación de nombrar un DPO, pero su encargado de tratamiento no. Por ejemplo, cuando el encargado solamente procese ciertos datos de la totalidad de los datos que el responsable recaba.

Un ejemplo de ello sería si el responsable es una empresa de salud que trata datos sensibles de sus pacientes, pero le encomienda al encargado de tratamiento solamente aquellos datos relacionados con sus proveedores de servicios de logística. En este caso, el responsable deberá nombrar un DPO, pero el encargado no.



Al contrario, puede suceder que un responsable no tenga obligación de nombrar un DPO debido a la naturaleza de las actividades que realiza pero contrata un encargado que sí tiene que nombrar un DPO debido al tipo de datos que procesa de otras empresas. Finalmente, cabría la posibilidad que ni el responsable de datos ni el encargado de tratamiento tengan la obligación de nombrar un DPO.

El artículo 37 del GDPR establece que los responsables o encargados de tratamiento deberán designar un DPO siempre que: "*a) el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función*

*judicial; b) las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala,* o *c) las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales (…) y de datos relativos a condenas e infracciones penales (…)*"[28].

En función del objeto de este trabajo, limitaré el análisis los incisos b y c del apartado 1 del artículo 37 que son los que aplican a la actividad privada. En consecuencia, dejaré de lado el primer inciso que hace referencia al sector público.

Para poder analizar correctamente qué empresas – dentro de las que están sujetas a regulación del GDPR - tienen obligación de nombrar un DPO deberemos revisar los conceptos de: (i) actividad principal; (ii) gran escala, (iii) observación habitual y sistemática; y (iv) datos especiales. Los cuatro conceptos son conceptos amplios que requieren algún nivel de aclaración dado que, en ciertos casos particulares, se pueden generar dudas sobre si una empresa deberá o no nombrar un DPO.

*a. Actividades principales*

El concepto de actividades principales es muy importante para poder entender en qué casos corresponderá o no a una empresa designar un DPO. El considerando 97 del GDPR establece que la actividad principal de una empresa está relacionada con "*sus actividades primarias y no están relacionadas con el tratamiento de datos personales como actividades auxiliares*".

[28] El subrayado me pertenece.

Según las Directrices, la actividad principal es aquella operación u operaciones clave y necesarias para lograr los objetivos de una empresa[29]. Puede ocurrir en algunos casos que, la actividad principal de un establecimiento esté directamente relacionada con el tratamiento de datos personales y en otros casos, no.

Por ejemplo, una empresa que procesa pagos electrónicos. Si bien su actividad principal es el procesamiento de pagos por vías electrónicas, no podría hacerlo sin procesar los datos de los pagadores y comercios.

Otro ejemplo, establecido por las Directrices es el caso de un hospital cuya actividad principal es prestar asistencia sanitaria. Si bien su actividad principal no consiste en procesar datos sino en prestar asistencia sanitaria, para poder llevar a cabo esa actividad, necesita procesar las historias clínicas y datos personales de los pacientes.

Distinto es el caso de una empresa dedicada a la fabricación de autos que es posible que tenga que tratar ciertos datos personales como por ejemplo aquellos de recursos humanos o proveedores. Sin embargo, ese tratamiento de datos no estará relacionado con la actividad principal de esa empresa y en consecuencia no tendrá la obligación de nombrar un DPO.

En este marco, autores como HUNTON & WILLIAMS entienden que aquellas actividades relacionadas con – por ejemplo - el tratamiento de datos vinculados a recursos humanos,

[29] Punto 2.1.2., Grupo de trabajo sobre protección de datos del artículo 29. "*Directrices sobre los delegados de protección de datos (DPD)*". WP 243 rev.01. Adoptadas el 13 de diciembre de 2016 y revisadas por última vez y adoptadas el 5 de abril de 2017. Disponible el 22 de febrero de 2020 en: https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf

proveedores, tecnología, video vigilancia, o monitoreo de correos electrónicos o de activos, no deberían considerarse como actividades principales. En consecuencia, no deberían implicar la designación de un DPO[30].

*b. Gran escala*

El concepto de gran escala no está definido en el GDPR. Será entonces muy importante analizar cada caso concreto para definir cuándo una empresa está haciendo un tratamiento a gran escala de datos personales y cuándo no.

El considerando 91 del GDPR establece que se incluirían en particular como operaciones a gran escala "*las operaciones de tratamiento a gran escala que persiguen tratar una cantidad considerable de datos personales a nivel regional, nacional o supranacional y que podrían afectar a un gran número de interesados y entrañen probablemente un alto riesgo*". Agrega también el considerando citado: "*el tratamiento de datos personales no debe considerarse a gran escala si lo realiza, respecto de datos personales de pacientes o clientes, un solo médico, otro profesional de la salud o abogado*"[31].

La descripción del considerando 91 detalla dos casos extremos en donde sí se trata de una operación a gran escala y resulta necesaria la designación de un DPO y el extremo donde no. Sin embargo, en el medio de estos dos extremos existen una cantidad de situaciones que deberán analizarse caso por caso.

[30] Hunton & Williams LLP – Centre for Information Policy Leadership (2016) "Ensuring the Effectiveness and Strategic Role of the Data Protection Officer under the General Data Protection Regulation" - GDPR Project DPO Paper, November 17, 2016

[31] Si bien este considerando 91 del GDPR ayuda a entender un poco más el concepto, es importante aclarar que tal considerando se refiere a la obligación de preparar evaluaciones de impacto relativas a la protección de datos y no a la designación de un DPO. En este sentido, y llegado el caso concreto, podría ocurrir que lo allí establecido no aplique al DPO y si a la evaluación de impacto.

Para ello, podrá ser útil tener en cuenta dos variables importantes. Estas dos variables son (i) la cantidad real de datos que se están tratando y, (ii) la cantidad relativa de esos datos que se están tratando en relación a la cantidad total de datos que en esa categoría de datos efectivamente exista.

Así las cosas, una empresa que procesa los datos de diez mil consumidores en un mercado de diez millones de consumidores, no pareciera ser un tratamiento a gran escala. Pero si se trata de los datos de diez mil consumidores de un segmento específico del mercado que tiene apenas quince mil, para ese mercado puntual, se trata de un tratamiento a gran escala.

En este sentido, las Directrices establecen ciertos parámetros a tener en cuenta para definir el concepto de gran escala. Estos parámetros son: (i) el número de potenciales afectados (como cifra concreta en función de una proporción respecto de una población específica), (ii) la cantidad o variedad de datos que se toman por persona; (iii) la duración o permanencia de la actividad de tratamiento de datos, y (iv) alcance geográfico[32].

Por otro lado, el concepto de gran escala debe analizarse en conjunto con el concepto de tratamiento habitual y sistemático que analizaremos a continuación. En este sentido se han expresado también las Directrices[33].

[32] Punto 2.1.3., Grupo de trabajo sobre protección de datos del artículo 29. "*Directrices sobre los delegados de protección de datos (DPD)*". WP 243 rev.01. Adoptadas el 13 de diciembre de 2016 y revisadas por última vez y adoptadas el 5 de abril de 2017. Disponible el 22 de febrero de 2020 en: https://ec.europa.eu/information society/newsroom/image/document/2016-51/wp243_en_40855.pdf

[33] Hunton & Williams LLP – Centre for Information Policy Leadership (2016) "Ensuring the Effectiveness and Strategic Role of the Data Protection Officer under the General Data Protection Regulation" - GDPR Project DPO Paper, November 17, 2016

*c. Observación habitual y sistemática de personas*

Tal como escribí en el párrafo anterior, el concepto de observación habitual y sistemática de personas debe darse también a gran escala. Es decir que, para nombrar un DPO, no alcanza con que haya una observación habitual y sistemática de datos, sino que – además - esa observación deberá ser a gran escala.

Se entiende que una actividad es habitual cuando se realiza en forma continuada, constante o periódica. Por otro lado, el término sistemático hace referencia a que la actividad se produce de acuerdo a un sistema o método creado especialmente para recabar y tratar los datos que serán sujetos a observación.

Las Directrices definen en qué casos se tratará de una observación habitual y sistemática de datos. Puntualmente, ocurre cuando la empresa en cuestión tenga una estrategia que consista en un "*sistema preestablecido, organizado o metódico que tiene lugar como parte de un plan general de recogida de datos*"[34].

Son ejemplos de observación habitual y sistemática de personas: operar una red de telecomunicaciones, redireccionar correos electrónicos, actividades de mercadotecnia basadas en datos, elaborar de perfiles y otorgar puntuación con fines 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,

[34] Punto 2.1.3., Grupo de trabajo sobre protección de datos del artículo 29. "*Directrices sobre los delegados de protección de datos (DPD)*". WP 243 rev.01. Adoptadas el 13 de diciembre de 2016 y revisadas por última vez y adoptadas el 5 de abril de 2017. Disponible el 22 de febrero de 2020 en: https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf

publicidad comportamental, seguimiento de los datos de bienestar, estado físico y salud mediante aplicaciones, etc. [35]

El concepto de observación habitual y sistemática incluye la creación de perfiles en internet, también con fines de publicidad comportamental pero no se limita al ecosistema *online*. En este marco, por ejemplo, un gimnasio que guarda las medidas corporales, el plan de alimentación y las actividades llevadas a cabo por sus clientes entra dentro de este concepto, así como también entran los supermercados u otras empresas que ofrecen tarjetas de descuentos.

Tal como sucede con el concepto de actividad principal y gran escala, dependerá de cada caso concreto. Así, el considerando 24 del GDPR establece que "*para determinar si se puede considerar que una actividad de tratamiento controla el comportamiento de los interesados, debe evaluarse si las personas físicas son objeto de un seguimiento en internet, inclusive el potencial uso posterior de técnicas de tratamiento de datos personales que consistan en la elaboración de un perfil de una persona física con el fin, en particular, de adoptar decisiones sobre él o de analizar o predecir sus preferencias personales, comportamientos y actitudes*".

*d. Categorías especiales de datos y datos relativos a condenas e infracciones penales*

La definición de categorías especiales de datos puede encontrarse en el mismo articulado del GDPR. El artículo 9 del GDPR establece que forman parte de categorías especiales

[35] Grupo de trabajo sobre protección de datos del artículo 29. "*Directrices sobre los delegados de protección de datos (DPD)*". WP 243 rev.01. Adoptadas el 13 de diciembre de 2016 y revisadas por última vez y adoptadas el 5 de abril de 2017. Disponible el 22 de febrero de 2020 en: https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf

de datos aquellos datos personales que revelen el origen étnico o racial de una persona, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física.

Por otro lado, el concepto de condenas e infracciones penales no requiere mucha explicación. Sin embargo, es importante destacar que, de conformidad con lo establecido por el artículo 10 del GDPR el tratamiento de datos personales relativos a condenas e infracciones penales "*sólo podrá llevarse a cabo bajo la supervisión de las autoridades públicas*" o cuando específicamente lo autorice la normativa de la Unión Europea o de alguno de sus estados[36].

Finalmente, es importante destacar que si bien el inciso c del artículo 37 del GDPR usa el vocablo "y" entre datos especiales y condenas o infracciones penales debería haberse utilizado el vocablo "o"[37]. Esto quiere decir que, para que exista la obligación de nombrar un DPO, no es necesario que la empresa trate categorías especiales de datos y datos relativos a infracciones penales, sino que alcanza con que la empresa trate alguna de las dos categorías de datos para tener la obligación de nombrar un DPO.

[36] El artículo 10 del GDPR puntualmente establece "*El tratamiento de datos personales relativos a condenas e infracciones penales o medidas de seguridad conexas sobre la base del artículo 6, apartado 1, sólo podrá llevarse a cabo bajo la supervisión de las autoridades públicas o cuando lo autorice el Derecho de la Unión o de los Estados miembros que establezca garantías adecuadas para los derechos y libertades de los interesados. Solo podrá llevarse un registro completo de condenas penales bajo el control de las autoridades públicas*".

[37] Las Directrices hablan directamente de "o" en lugar de "y" (punto 2.1.c).

ii. DPO voluntario y otros responsables de datos

Como destaqué al principio de este trabajo, uno de los principios rectores del GDPR es el principio de responsabilidad proactiva por lo que cada empresa debe evaluar qué medidas tomar para hacer más eficiente el cumplimiento del GDPR y de los principios allí establecidos en materia de protección de datos. Siguiendo este principio, el artículo 37 inciso 4 del GDPR establece que aun cuando no resulte obligatorio nombrar un DPO las empresas podrán designar uno por lo que es posible que sin perjuicio de no estar obligadas, las empresas igualmente decidan nombrar un DPO[38].

Las razones para nombrarlo pueden ser muchas y variadas, podría ser ejemplo por temas reputaciones tal como sostiene ROSS[39]. O bien podría ser porque la dirección de la empresa siguiendo el principio de responsabilidad activa considere importante nombrarlo, tal como destacamos antes.

Por otro lado, las Directrices establecen que cuando la obligación de designar un DPO no es evidente, es recomendable documentar todo el análisis interno llevado a cabo por la empresa para llegar a tal conclusión. En este sentido, y en función del principio de

[38] El inciso 4 del artículo 37 del GDPR establece: "*En casos distintos de los contemplados en el apartado 1, el responsable o el encargado del tratamiento o las asociaciones y otros organismos que representen a categorías de responsables o encargados podrán designar un delegado de protección de datos o deberán designarlo si así lo exige el Derecho de la Unión o de los Estados miembros. El delegado de protección de datos podrá actuar por cuenta de estas asociaciones y otros organismos que representen a responsables o encargados*". Por su parte, vale recordar que el apartado 1 establece: "*El responsable y el encargado del tratamiento designarán un delegado de protección de datos siempre que: a) el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial; b) las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala, o c) las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales con arreglo al artículo 9 y de datos relativos a condenas e infracciones penales a que se refiere el artículo 10*".

[39] Ross David, GDPR and the Role of the Data Protection Officer. Octubre 1, 2018. Disponible el 2 de febrero de 2020 en http://www.rmmagazine.com/2018/10/01/gdpr-and-the-role-of-the-data-protection-officer/

responsabilidad proactiva, es posible también que cuando no sea clara la designación de un DPO para una empresa en particular, tal empresa decida de todas maneras designarlo.

Las empresas que no están obligadas a nombrar un DPO pero que tengan intención de hacerlo, podrán evaluar dos alternativas distintas. Por un lado, la de designar un DPO voluntario y, por el otro, la de designar algún otro responsable de datos que no sea estrictamente un DPO.

Respecto del DPO voluntario, vale decir que se ha discutido si nombramiento implica que tal DPO tenga las mismas obligaciones y estatus que el DPO obligatorio. Es decir, que se le apliquen las mismas normas, roles y responsabilidades establecidas en el GDPR para los DPO.

Las Directrices no establecen nada al respecto y las posturas sobre la cuestión varían[40]. Por un lado, HUNTON & WILLIAMS hacen referencia a que debería entenderese que, si una empresa que no está obligada bajo el GDPR a nombrar un DPO decide hacerlo de todas maneras, tal DPO tendrá el mismo estatus que el DPO obligatorio regulado por el GDPR.

Para HUNTON & WILLIAMS esta postura tiene como fundamento el hecho de que, si tal DPO no tuviera las mismas cualidades que el DPO del GDPR, podría confundirse su rol. Esta confusión del rol podría ocurrir tanto dentro de la empresa, entre los empleados, directivos y el propio responsable respecto de su propio rol, como también afuera de ella, frente a los titulares de los datos y a la autoridad de aplicación.

[40] Hunton & Williams LLP – Centre for Information Policy Leadership (2016) "Ensuring the Effectiveness and Strategic Role of the Data Protection Officer under the General Data Protection Regulation" - GDPR Project DPO Paper, November 17, 2016

En sentido contrario, podría entenderse que el responsable de datos voluntario no debería tener los mismos derechos y obligaciones del GDPR. Ello argumentando que si aun sin tener la obligación, una empresa nombra un DPO tal persona no debería tener el cargo de DPO en términos del GDPR en tanto no está obligado a nombrarlo bajo el GDPR.

En mi opinión si una empresa a la que le aplica el GDPR decide, por la razón que sea, nombrar un responsable de protección de datos y a tal responsable le pone el nombre de DPO, ese DPO no podrá ser uno distinto al DPO del GDPR y se le aplicarán sus normas. De lo contrario y tal como ya resalté, se podría confundir su rol - no solo dentro de la organización - sino frente a los titulares de los datos y a la propia autoridad de aplicación.

Finalmente, puede pasar que una empresa a la que le aplica el GDPR, pero sin obligación de nombrar un DPO decida nombrar algún responsable de protección de datos que no tenga las mismas obligaciones y estatus que el DPO. Las razones pueden ser varias: porque la legislación de un país que no forme parte de la Unión Europea donde opere así lo requiera, porque aun cuando no tenga obligación de nombrar un DPO necesite a alguna persona que esté a cargo de los temas de protección de datos, porque es parte de su política interna, entre muchas otras.

En este caso, y en función de lo escrito más arriba, es recomendable que el cargo que ocupe esa persona no tenga el nombre de DPO a fin de que no se lo confunda con el DPO – obligatorio o voluntario - del GDPR. En este sentido, podrá denominarse, por ejemplo, responsable de datos personales, gerente de datos, etc. pero no “delegado de protección de datos”.

Es recomendable a su vez que las tareas que desempeñe tal persona a cargo de temas de privacidad en una empresa estén claramente delimitadas y puedan distinguirse del DPO. Así, la descripción de su trabajo debe decir que no se trata de un DPO y, aún más, las búsquedas de trabajo deben decir específicamente que no se trata de un cargo de DPO.

iii. Grupos empresarios

El GDPR permite la designación de un solo DPO para varias organizaciones que formen un grupo empresario cuando el DPO "*sea fácilmente accesible desde cada establecimiento*". Es importante en consecuencia, analizar el concepto de "accesible" para entender como cumplirlo.

Sin perjuicio de un mayor análisis que haré más adelante sobre la accesibilidad del DPO, a esta altura vale destacar que el concepto de accesibilidad del DPO debe estudiarse desde dos aspectos distintos. Por un lado, que sea fácil contactar al DPO por parte de los titulares de los datos y las autoridades de aplicación -con independencia del lugar en que residan cada una de las partes; y, por otro lado, que el DPO tenga acceso dentro de la organización a toda la información necesaria para cumplir con su rol.

Respecto del segundo aspecto, la accesibilidad implica también el acceso a las formas en que se recaban los datos personales y los procesos de tratamiento. Para ello, el DPO deberá tener acceso a los contratos que suscriba la empresa para subcontratar el procesamiento de datos por ejemplo, contratos de software o hardware, contratos de almacenamiento de datos, de sistemas de gestión, de sistemas de seguridad, etc.[41]

[41] Lambert, P. (2017). The Data Protection Officer. New York: Auerbach Publications, capítulo 2 https://doi.org/10.1201/9781315396743

Cuando el grupo empresario sea muy grande, las herramientas tecnológicas que permitan al DPO acceso a todas las filiales de la empresa será muy importante. El DPO podrá, además, nombrar a un equipo que lo asista en su rol y cuyos miembros estén ubicados en cada uno de los países donde la empresa opera de manera de tener contacto directo con cada una de las seccionales.

**C. Características personales del DPO**

Analizaré en el primer apartado de esta sección, qué cualidades personales deben tenerse en cuenta a la hora de designar un DPO. Haré también una breve referencia a la posibilidad de designar a una organización externa a la empresa para que ocupe el rol de DPO y qué cuestiones deben tenerse en cuenta a la hora de optar por esa solución.

i. Cualidades profesionales del DPO

El artículo 37, inciso 5 del GDPR establece que el DPO "*será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones*". Tales funciones son las establecidas en GDPR para el DPO y las analizaré más abajo en este trabajo.

El DPO deberá entonces tener conocimientos en temas de protección de datos tales como los conceptos de privacidad desde el diseño, por defecto y seguridad de datos. Sin embargo, el considerando 97 del GDPR agrega una cuestión más y establece que "*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 la empresa en cuestión.

Así, no alcanza únicamente con que el DPO conozca la legislación aplicable en materia de protección de datos, sino que se requiere además que el DPO conozca el negocio de la empresa en la que trabaja y esté familiarizado con el tipo de datos que procesa tal empresa. Es más, se ha sostenido que no es indispensable que el DPO tenga una formación académica en leyes en la medida en que, (i) pueda capacitarse en ese aspecto y (ii) tenga acceso a abogados expertos que puedan asistirlo en la materia.

Resulta importante entonces que, además del conocimiento legal requerido, el DPO tenga otras herramientas que le permitan desarrollar integralmente sus funciones. Entre esas herramientas se destacan las herramientas y conocimientos tecnológicos, éticos, de auditoría y de comunicación que pueda tener un DPO.



El DPO deberá también tener habilidades para trabajar en equipo, delegar tareas y responsabilidades, contratar expertos en temas específicos, preparar informes y reportes y mantener una buena relación con las autoridades de aplicación de cada país. Finalmente, será fundamental que el DPO tenga la capacidad de cambiar o mejorar la cultura de la organización a la que pertenece a una cultura de protección de datos.

Es importante destacar que cuanto más grande sea la empresa y más complejas sean las categorías de datos que se manejen, mayor será el grado de experiencia requerido para ese DPO. En igual sentido, cuanto mayor sea el riesgo asociado a la cantidad y tipo de

datos que se tratan, mayor será el nivel de experiencia que deberá tenerse en cuenta a la hora de designar un DPO.

Así, si se trata de una empresa dedicada al rubro de la salud que maneja categorías especiales de datos, el nivel de experiencia requerido para el DPO será mayor. En cambio, el nivel de experiencia requerido para un DPO será menor para una empresa que presta un servicio público y que maneja datos de gran cantidad de usuarios pero que esos datos no incluyen categorías especiales de datos.

Finalmente, si bien existen ciertos cursos y certificaciones otorgadas por instituciones educativas y por las propias autoridades de aplicación de ciertos países, el GDPR no exige que los DPO obtengan una certificación específica. Sin embargo, y en función del principio de responsabilidad proactiva, las empresas podrán exigir a los candidatos a DPO algún tipo de certificación o bien, incentivar al DPO y a las personas que trabajen en su equipo a que hagan cursos y capacitaciones relativas a la protección de datos.



ii. Tipos de DPO

El artículo 37 inc. 6 del GDPR establece que "*el delegado de protección de datos podrá formar parte de la plantilla del responsable o del encargado del tratamiento o desempeñar sus funciones en el marco de un contrato de servicios*". Así, una empresa puede optar entre designar a alguien para que ejerza el rol de DPO dentro de su organigrama o subcontratar una firma especializada en estos temas.

La elección entre un DPO interno y otro externo dependerá en cierta medida de: (i) el tamaño de la empresa y (ii) la necesidad de horas de trabajo que demande ese cargo. Así,

es posible que una empresa grande requiera de un DPO dentro de su nómina de empleados en forma permanente y que- además- este DPO tenga un equipo a cargo mientras que un *start-up* o una empresa mediana con poco procesamiento de datos prefiera designar una empresa especializada para que ocupe ese rol y que pueda dedicarse en forma *part-time* a esa tarea.

En el caso de que se decida contratar una organización externa para que ocupe el cargo de DPO, deberá verificarse que todos los miembros a cargo del equipo que asistirá a tal empresa en el rol de DPO estén capacitados para hacerlo en la forma que detallé en el apartado anterior. Por otro parte, sería recomendable además establecer dentro del equipo a cargo de cada empresa, una persona humana responsable que será quién tenga a su cargo la relación no solo con la empresa que los haya contratado sino también con las autoridades de aplicación y con los titulares de los datos.

En caso de designar a una organización externa para que ocupe el rol de DPO de una empresa, será importante confirmar que no exista ningún conflicto de interés entre esa organización y la empresa que los contrata. Esto pensando por ejemplo en aquellos casos donde la empresa contratada sea también DPO de, por ejemplo, la competencia.

Finalmente, y como escribí anteriormente, cuando el DPO está a cargo de una persona interna de la empresa es posible designar un equipo a cargo del DPO para llevar a cabo todas las funciones del DPO. En ese caso, los miembros del equipo pueden tener distintas profesiones de manera que se puedan cubrir todas las áreas necesarias para cumplir con eficiencia el rol del DPO, ello sin perjuicio de que el DPO será uno solo y el responsable del equipo.

**D. Rol del DPO**

Los artículos 38 y 39 del GDPR regulan la posición y funciones del DPO. Analizaré en primer lugar cada una de las funciones a cargo del DPO para luego analizar algunos puntos más controvertidos e interesantes relativos a la función del DPO, entre ellos pondré especial atención a los conceptos de: (i) accesibilidad, (ii) independencia, y (iii) confidencialidad y conflicto de interés.

i. Actividades a cargo

El artículo 39 del GDPR establece que serán las principales funciones del DPO: (i) velar por el cumplimiento del GDPR por parte de la empresa y sus empleados; y (ii) intermediar entre las autoridades de control y la empresa[42]. Esto implica, entre otras cosas, capacitar a los empleados, informar inmediatamente a los órganos que toman decisiones sobre cualquier incumplimiento a las estipulaciones del GDPR, informar a la empresa sobre cambios normativos, monitorear los procesos, colaborar con la confección de la evaluación de impacto relativa a la protección de datos, etc.[43].



[42] El artículo 39 del GDPR puntualmente establece que el DPO tendrá las siguientes funciones: "*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 GDPR y de otras disposiciones de protección de datos de la Unión Europea o de los estados miembros; b) supervisar el cumplimiento de lo dispuesto en el GDPR, de otras disposiciones de protección de datos de la Unión Europea 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 (…); d) cooperar con la autoridad de control; y e) actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, (…), y realizar consultas, en su caso, sobre cualquier otro asunto".*

[43] Ross David, GDPR and the Role of the Data Protection Officer. Octubre 1, 2018. Disponible el 2 de febrero de 2020 en http://www.rmmagazine.com/2018/10/01/gdpr-and-the-role-of-the-data-protection-officer/

Para poder llevar a cabo estas funciones, se requiere de un cambio cultural en la organización que permita analizar todos los procesos a la luz del GDPR. Este cambio cultural es un mandato del propio GDPR que instaura los principios de protección de datos desde el diseño o *privacy by disign* y por defecto o *privacy by default*[44].

Analizar los conceptos de privacidad desde el diseño y por defecto excedería ampliamente este trabajo. Sin embargo, es importante destacar que, el concepto de privacidad desde el diseño implica que las organizaciones asuman que - en todo momento - desde el comienzo y hasta la terminación de cualquier proceso dentro de la organización, las decisiones deben tomarse a la luz de la normativa sobre protección de datos.

[44] El considerando 78 del GDPR establece que: "*La protección de los derechos y libertades de las personas físicas con respecto al tratamiento de datos personales exige la adopción de medidas técnicas y organizativas apropiadas con el fin de garantizar el cumplimiento de los requisitos del presente Reglamento. A fin de poder demostrar la conformidad con el presente Reglamento, el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto. Dichas medidas podrían consistir, entre otras, en reducir al máximo el tratamiento de datos personales, seudonimizar lo antes posible los datos personales, dar transparencia a las funciones y el tratamiento de datos personales, permitiendo a los interesados supervisar el tratamiento de datos y al responsable del tratamiento crear y mejorar elementos de seguridad. Al desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que están basados en el tratamiento de datos personales o que tratan datos personales para cumplir su función, ha de alentarse a los productores de los productos, servicios y aplicaciones a que tengan en cuenta el derecho a la protección de datos cuando desarrollan y diseñen estos productos, servicios y aplicaciones, y que se aseguren, con la debida atención al estado de la técnica, de que los responsables y los encargados del tratamiento están en condiciones de cumplir sus obligaciones en materia de protección de datos. (...)*"
Por otro lado, el artículo 25 del GDPR que regula la protección de datos desde el diseño y por defecto establece: "*1.Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados. 2.El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas*".

Este cambio de perspectiva, que implica no solo que todos los procesos estén diseñados desde la óptica de protección de datos sino también que cada uno de los miembros de la organización realice su trabajo desde esta óptica, implica el cambio cultural al que estoy haciendo referencia. El DPO es, en gran medida, el responsable de que este cambio cultural pueda realizarse dentro de la organización.

Para ello, el GDPR exige que el DPO – y su equipo – puedan (i) revisar y participar en todos los procesos ya existentes y en los nuevos que vayan apareciendo y que tengan relación con el tratamiento de datos; y (ii) participar desde el principio en aquellas nuevas actividades que se pretendan llevar a cabo y que contengan algún aspecto relativo al tratamiento de datos personales[45].

En relación al primer punto, la empresa debe garantizar no solo que el DPO y su equipo tengan acceso constante a los procesos de tratamiento de datos. Se debe garantizar también que cualquier empleado pueda contactarse con el DPO y su equipo para evacuar dudas o consultas en relación a este tema.

El segundo punto implica que la empresa tiene que garantizar desde el principio y mediante mecanismos que en lo posible estén estandarizados, el acceso o consulta al equipo del DPO de los nuevos proyectos que se lancen. Esto justamente para que cada proyecto que pretenda lanzarse de analice, desde su inicio, a la luz de la normativa sobre protección de datos.

[45] Artículo 38 inciso 1 del GDPR.

Para poder lograr estos objetivos, las Directrices[46] establecieron ciertos ejemplos que deberían intentar llevar a cabo las organizaciones para garantizar que el DPO pueda desarrollar correctamente sus funciones. Entre ellos se destacan: (i) la participación del DPO con regularidad en reuniones con los cuadros directivos altos y medios; (ii) la participación del DPO cuando se toman decisiones con implicaciones para la protección de datos; (iii) la documentación adecuada de los casos en que no se decida seguir la recomendación del DPO; y (iv) la asignación de recursos adecuados para el cumplimiento de las funciones del DPO y su equipo.

Finalmente, resulta conveniente que el DPO lleve un registro de operaciones de la empresa y de todas las medidas que, durante se función, se implementen para cumplir con la normativa de protección de datos. Esto le servirá no solo para tener un control interno de las actividades llevadas a cabo por la empresa en el marco del GDPR sino también como documento de respaldo para cualquier interacción entre la empresa y las autoridades de control.



ii. Accesibilidad y ubicación del DPO

El artículo 37, inciso 7 del GDPR establece que "*el responsable o el encargado del tratamiento publicarán los datos de contacto del [DPO] y los comunicarán a la autoridad de control".* Por otro lado, y como escribí más arriba, el artículo 37 inciso 2 establece a su vez que, un grupo empresarial podrá designar un solo DPO para todo el grupo en la medida en que tal DPO "*sea fácilmente accesible desde cada establecimiento*".

[46] Punto 3.1., Grupo de trabajo sobre protección de datos del artículo 29. "*Directrices sobre los delegados de protección de datos (DPD)*". WP 243 rev.01. Adoptadas el 13 de diciembre de 2016 y revisadas por última vez y adoptadas el 5 de abril de 2017. Disponible el 22 de febrero de 2020 en: https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf

El objetivo del GDPR en lo que respecta a la accesibilidad del DPO tiene que ver no solo con la posibilidad de que la autoridad de control tenga acceso al DPO. Se busca también que los titulares de los datos y los empleados y funcionarios de la empresa puedan contactarlo.

En este sentido, el artículo 38 inciso 4 del GDPR establece que los titulares de los datos "*podrán ponerse en contacto con el [DPO] por lo que respecta a todas las cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos*". Esta accesibilidad tiene que ser efectiva, es decir que de hecho debe existir alguna forma de contacto simple y eficaz con el DPO o- en su defecto y tal como desarrollo más abajo- con algún miembro del equipo del DPO.

En igual sentido, el deber de publicar los datos de contacto del DPO no se limita a la información que deberá darse a la autoridad de control del país de la Unión Europea donde tenga asiento la empresa que nombre un DPO. En el caso de empresas argentinas que no tengan asiento en ningún país de la Unión Europea pero que deben nombrar un DPO en los términos del GDPR, deberá publicar en su página web, algún medio de contacto con el DPO.

Por otro lado, el deber de publicar los datos de contacto implica también notificar a los propios empleados de la empresa para que todos puedan contactar al DPO para cualquier eventualidad relacionada con el tratamiento de datos. Se puede incluso crear algún tipo de canal de comunicación que permita a los empleados hacer denuncias anónimas sobre temas de protección de datos al DPO.

Es evidente que en aquellas empresas con presencia en diversos países o con altos niveles de tratamiento de datos (v.g. una empresa global de consumo masivo a través de ventas *online*), el DPO no podrá resolver en forma personal cada uno de los casos y estar en todos los lugares a la vez. Sin embargo, la empresa deberá garantizar que el DPO pueda designar un equipo que le reporte directamente y que pueda hacer frente inmediatamente a cualquier consulta o requerimiento en el país donde tal consulta o requerimiento se genere.

Desde el punto de vista geográfico y a fin de salvar las distancias, será importante el uso de sistemas de comunicación que permitan al DPO participar remotamente de reuniones o situaciones que requieran su presencia. Sin perjuicio de ello, quién ocupe el cargo de DPO de una empresa con presencia en muchos países, deberá estar disponible para viajar periódicamente a los distintos países donde la empresa tenga filiales o – dependiendo del caso - las veces que haga falta.



Se ha discutido si, desde la óptica del GDPR es necesario que el DPO tenga su asiento permanente en algún país de la Unión Europea. El GDPR no tiene una prescripción específica al respecto y resulta fundamental analizarlo para el caso de empresas argentinas.

Las Directrices recomiendan que el DPO esté ubicado en la Unión Europea[47]. Sin embargo se ha sostenido también[48] – y coincido con esta postura – que lo lógico es que el DPO tenga sus oficinas en el país principal de la empresa, independientemente de si ese país forma parte o no de la Unión Europea.

Esta postura me parece razonable sobre todo en aquellos casos en que una empresa ni siquiera tiene filiales en la Unión Europea. No tendría ningún sentido instalar oficinas allí al solo efecto de que el DPO pueda instalarse cuando toda la actividad de la organización ocurre en otro lugar.

En un caso así, será fundamental que la empresa garantice la accesibilidad del DPO en todo momento a los casos ubicados dentro del territorio de la Unión Europea. Y que, sobretodo, facilite el contacto con las autoridades de aplicación.



iii. Independencia del DPO

La independencia del DPO es una de las características más relevantes de su función. El GDPR en su artículo 38 regula algunas pautas que tienden a garantizar tal independencia.

Puntualmente el GDPR establece que la empresa deberá garantizar que el DPO (i) "*participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales*" (art. 38 inc. 1); (ii) tenga acceso a los recursos que

[47] Punto 2.4, Grupo de trabajo sobre protección de datos del artículo 29. "Directrices sobre los delegados de protección de datos (DPD)". WP 243 rev.01. Adoptadas el 13 de diciembre de 2016 y revisadas por última vez y adoptadas el 5 de abril de 2017. Disponible el 22 de febrero de 2020 en: https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf

[48] Hunton & Williams LLP – Centre for Information Policy Leadership (2016) "Ensuring the Effectiveness and Strategic Role of the Data Protection Officer under the General Data Protection Regulation" - GDPR Project DPO Paper, November 17, 2016

fueran necesarios para desempeñar su función (art. 38 inc. 2); (iii) "*no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones*" (art. 38 inc. 3); (vi) no sea "*destituido ni sancionado (…) por desempeñar sus funciones*" (art. 38 inc. 4); y (v) responda directamente el nivel jerárquico de la empresa (art. 38 inc. 4).

En el apartado d.i de este trabajo ya analicé lo establecido en el inciso 1 del artículo 38 sobre el acceso a todas las cuestiones relativas a la protección de datos personales en la empresa por lo que, en honor a la brevedad, remito a lo que allí escribí. Lo único que quisiera agregar ahora es que, como parte del cambio cultural que una empresa debe hacer a la luz del concepto de protección de datos, se debe intentar que el DPO no sea visto internamente como un auditor-policía que no permite llevar a cabo las distintas actividades o proyectos que una empresa quiere hacer.

Debería, en cambio, verse como como aquel referente en materia de datos a quién se pueda consultar en caso de duda y recurrir ante cualquier inconveniente, filtración o incumplimiento de las normas en materia de protección de datos[49]. Otorgarla acceso al DPO en estos términos es uno de los desafíos más grandes en relación a la figura del DPO.

Las funciones del DPO por un lado incluyen tareas de auditoría, pero también tienen un gran componente de gestión. Esta gestión implica no solo aplicar y hacer cumplir el GDPR sino también generar el cambio de cultural empresarial hacia la protección de datos al que ya tantas veces hice referencia.

[49] Hunton & Williams LLP – Centre for Information Policy Leadership (2016) "Ensuring the Effectiveness and Strategic Role of the Data Protection Officer under the General Data Protection Regulation" - GDPR Project DPO Paper, November 17, 2016

Así, las empresas y el propio DPO deberán buscar la manera de que el DPO, en lugar de ser percibido como un policía "que no nos deja hacer nada", pueda ser percibido como un aliado que "nos ayuda a hacer las cosas bien". El DPO debe ser visto dentro de la organización como aquella persona a quién consultar para solucionar o encarar temas de datos y no a alguien que - aún en forma inconsciente – se trate de esconder la forma de trabajar en lo relativo a temas de datos.

El inciso 2 del artículo 38 tiene que ver con los recursos que se le destinan al DPO para que pueda realizar sus funciones. El presupuesto que se le asigne al DPO debe ser suficiente para llevar a cabo sus tareas en forma eficaz y efectiva.

A mayor complejidad en el procesamiento de datos, mayor será la cantidad de recursos que la empresa deberá destinar al desarrollo de las funciones del DPO. La independencia, desde el punto de vista presupuestario, tiene que ser no solo financiera sino también de recursos humanos y de tiempo disponible para llevar a cabo sus tareas.

Este presupuesto debe incluir capacitaciones, viajes y acceso a tecnología, equipamiento e infraestructura. Adicionalmente, el presupuesto debe contemplar la posibilidad de contratar servicios externos que le permitan al DPO desarrollar sus tareas (servicios legales, por ejemplo).

Como ya desarrollé más arriba, el DPO debe tener la posibilidad de contratar los recursos humanos que sean necesarios para asistirlo en sus tareas. Dependiendo del tamaño de la

empresa y la complejidad de los datos que se procesan, será el tamaño del equipo del DPO pudiendo incluso no ser necesario que exista tal equipo.

En otros casos en cambio, el equipo deberá ser interdisciplinario para cubrir todas las necesidades de la empresa. Puede ocurrir incluso que el equipo del DPO esté localizado en las distintas sucursales de la empresa y aún disperso en distintos países o continentes.

El inciso 3 del artículo 38 del GDPR que analizaremos a continuación tiene que ver con el hecho de que las empresas deben garantizar que el DPO no reciba ningún tipo de orden o instrucción en lo que respecta a sus funciones como DPO. Al respecto, el considerando 97 del GDPR establece que "*sean o no empleados del responsable del tratamiento, deben estar en condiciones de desempeñar sus funciones y cometidos de manera independiente*".

En consecuencia, la empresa no puede interferir en la forma en que trabaja el DPO respecto de la implementación e interpretación del GDPR. Sin embargo, es importante señalar que esta independencia en la toma de decisiones respecto de sus funciones se limita solamente a lo que tiene que ver con la aplicación y cumplimiento del GDPR en la empresa, es decir en lo que respecta al rol de DPO.

En aquellos casos donde el DPO es interno, sigue siendo un empleado de la empresa y, en consecuencia, es lógico que tenga que atenerse a las decisiones jerárquicas que tengan que ver con todos aquellos temas distintos a su rol de DPO (por ejemplo normas de convivencia, vacaciones, etc.). A su vez, si el DPO ocupa además otras funciones dentro

de la organización – es por ejemplo el gerente de legales – sí podrá recibir instrucciones de parte de la empresa sobre cómo realizar sus funciones en tanto gerente de legales.

Por otro lado, si bien en lo que respecta a sus funciones en relación al GDPR el DPO es independiente, eso no lo exime de la obligación de rendir cuentas del trabajo realizado y la forma en que se llevó a cabo. Esta rendición de cuentas deberá hacerse a las máximas autoridades de la empresa.

La primera parte del inciso 4 del artículo 38 del GDPR hace referencia a la imposibilidad de que el DPO sea sancionado por las decisiones que tome en relación a la política de protección de datos que implemente para esa empresa. Así, por ejemplo, no se podría despedir o sancionar a un DPO porque recomendó no avanzar con un determinado proyecto porque tal proyecto implicar una violación al GDPR o un riesgo alto a la privacidad de los titulares de los datos.

El GDPR no establece en qué casos sí se puede despedir o sancionar a un DPO. Al respecto, entiendo que, si el DPO no cumpliera adecuadamente sus funciones, por ejemplo, sin resolver quejas de titulares, sin colaborar con la autoridad de aplicación o sin participar – aunque se lo invite- en la toma de decisiones relativas a sus funciones, la empresa podría desvincularlo.

Sin embargo, coincido con ciertos autores como LAMBERT[50] que puede resultar muy difícil definir la razón de la sanción. En este sentido, puede ser complicado distinguir en qué casos se está sancionando o despidiendo a un DPO por su mala gestión y que tal mala

[50] Lambert, P. (2017). The Data Protection Officer. New York: Auerbach Publications, capítulo 2 https://doi.org/10.1201/9781315396743

gestión no esté directamente relacionada con una opinión o punto de vista emitido por el DPO respecto de un tema puntual sobre protección de datos.

Finalmente, la segunda parte del inciso 4 del artículo 38 hace referencia a la necesidad de que el DPO responda al nivel jerárquico de la empresa. Sobre este punto, vale la pena resaltar lo que se detalla a continuación.

Por un lado, el hecho de que el DPO tenga acceso directo a los rangos más altos de una empresa, hace suponer que el rol del DPO está reservado para personas con cierto nivel de experiencia que sepan cómo manejarse frente a las posiciones jerárquicas. Debe entenderse además por nivel jerárquico aquellas personas que tiene capacidad para tomar decisiones sobre aquellas cuestiones que conciernen a las funciones del DPO.

Así, dependerá mucho de cada empresa quién ocupe ese cargo, pero dependerá también del tema que se deba decidir. Por ejemplo, si de lo que se trata es de implementar un nuevo sistema de gestión de los datos de los empleados, es posible que cualquier situación relativa a la implementación de tal sistema deba analizarse con el responsable de recursos humanos y no con el presidente del directorio que, por su posición jerárquica dentro de la organización, es probable que no esté al tanto de los detalles de tal proceso.

En otro ejemplo, si el tema a decidir tuviera que ver con una filtración de datos masiva sobre información de clientes de la compañía, es posible que sí haya que acceder al presidente de la empresa. Esto porque, aún si la cuestión fuera competencia de un gerente operativo o comercial, su gravedad podría merecer el contacto con alguien de mayor jerarquía.

En definitiva, dependerá de cada caso puntual a quién deberá acceder el DPO para la toma de decisiones. En algunos casos será el directorio, en otras será el gerente general o el gerente financiero, etc.

En otros casos, dependiendo de cada situación específica, puede pasar que el DPO en algún momento requiera tener un contacto directo con el directorio y a su vez con los gerentes medios. Lo importante es que siempre tenga acceso a quién tome tales decisiones.

Por otro lado, y tal como escribí en mi segundo ejemplo más arriba, es mi opinión que no cualquier situación debe ser reportada a los cargos jerárquico sino solamente aquellas que, por su naturaleza o gravedad requieran de la toma de decisiones por parte de las personas con capacidad para tomar decisiones. Dependerá entonces del DPO definir en qué situaciones vale la pena contactar a los cargos directivos y cuando no.



En este sentido, es importante destacar que en general, los puestos jerárquicos de una empresa no tienen ni el tiempo ni la experiencia en materia de datos requerida para poder analizar todas las cuestiones de privacidad vinculadas al desarrollo de los negocios de la empresa. Se deberá entonces garantizar que, cuando el DPO lo considere pertinente, pueda acceder a las personas que toman las decisiones.

Finalmente, quisiera entonces resaltar lo difícil que puede llegar a ser para una empresa nombrar a una persona en un puesto de DPO que tenga todas estar particularidades relativas a su independencia, no solo desde el punto de vista presupuestario, pero sino

también desde el punto de vista laboral, por ejemplo, a la hora de dar una devolución de desempeño. Por otro lado, si la empresa no facilita todos estos extremos para el cargo del DPO, difícilmente el DPO pueda realizar su trabajo conforme se lo exige el GDPR[51].

iv. Confidencialidad y conflictos de interés del DPO

Otra de las características distintivas de la función del DPO está relacionada con su deber de confidencialidad y los conflictos de interés que se pueden suscitarse alrededor de su cargo. En este sentido, el artículo 38 *in fine* del GDPR establece que el DPO "*estará obligado a mantener el secreto o la confidencialidad en lo que respecta al desempeño de sus funciones"* y que podrá desempeñar otras funciones en la medida en que la empresa garantice que "*dichas funciones y cometidos no den lugar a conflicto de intereses*".

Las personas que ocupen el cargo de DPO dentro de una organización, tendrán pleno acceso a gran cantidad de información confidencial respecto de la forma en que se recaban y procesan los datos. Tendrán además acceso a secretos comerciales, datos de clientes y productos y demás información clave para la empresa.

En este marco, el DPO debe guardar estricta confidencialidad respecto de toda esa información. Esto en tanto el deber de confidencialidad es parte de su deber de fidelidad hacia la organización para la que trabaja.

El deber de confidencialidad es claro cuando se trata de no divulgar la información a terceros ajenos a la empresa. Sin embargo, genera ciertos conflictos en dos situaciones:

[51] Ross David, GDPR and the Role of the Data Protection Officer. Octubre 1, 2018. Disponible el 2 de febrero de 2020 en http://www.rmmagazine.com/2018/10/01/gdpr-and-the-role-of-the-data-protection-officer/

(i) respecto de la información recabada por el DPO dentro de la empresa y el deber de reporte al personal jerárquico y (ii) respecto de la relación del DPO con las autoridades de aplicación.

En relación al primer punto, forma también parte de las funciones del DPO resaltar aquellas cuestiones que estén sucediendo en contravención con lo establecido por el GDPR lo que podría entenderse como una afectación al principio de confidencialidad. En este marco, bien podrían los empleados de la organización negarle al DPO cierta información por miedo a sea reportada a los altos mandos.

Será entonces importante generar sistemas de reporte que permitan que el DPO tenga acceso a toda la información necesaria para poder cumplir con su deber. Estos sistemas de reporte pueden ser varios y distintos, desde una línea de llamadas anónimas a un mail donde puedan hacerse denuncias o directamente la posibilidad de hablar con el DPO, entre otros.



Por otro lado, el DPO tiene también obligación de "*cooperar con la autoridad de control y actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento*" de datos. En este caso, se deberá tener en cuenta también el deber de lealtad que el DPO tiene frente a la empresa para la que trabaja de manera de no divulgar información más allá de lo requerido por el GDPR y la ley para no exponer la información confidencial de la empresa.

En cualquiera de los dos casos, es fundamental que desde la organización se perciba al DPO como una persona a quién se puede y debe consultar y que asistirá a cada uno de los

miembros de la empresa a desarrollar mejor su trabajo. No debe entenderse al DPO como una persona que reporta las malas acciones, sea internamente a los superiores o externamente a la autoridad de control.

Al contrario, el DPO debe ser una persona que resuelve conflictos y ayuda a evitar potenciales riesgos internamente. Siendo además quién, puertas afuera de la empresa, busca mantener un diálogo amigable y cooperante con las autoridades de control.

En relación a los conflictos de interés que puedan llevarse a cabo alrededor del cargo de DPO, es importante destacar que el GDPR no prohíbe que el DPO de una empresa pueda, además, tener otras funciones si su tamaño y la complejidad del tratamiento de datos que se realice lo permite. Sin embargo, deberán tenerse especialmente en cuenta que ciertos puestos podrían generar un conflicto de interés en la persona del DPO a la hora de tomar una decisión para hacer cumplir el GDPR.



Así, ciertos cargos sobretodo gerenciales como por ejemplo aquellos relacionados con producto, ventas, finanzas o tecnología pueden en algunos casos afectar el desarrollo de la función del DPO tal como está establecida en el GDPR. Por otro lado, cuando la persona que tenga el cargo de DPO tiene además otro cargo dentro de la empresa en cuyo caso será muy importante que se asigne tiempo suficiente a las funciones de DPO para por llevarlas a cabo.

iv. Alcance de la responsabilidad

El artículo 24 del GDPR hace responsables por el incumplimiento de sus prescripciones al encargado o responsable del tratamiento de los datos y no al DPO. De hecho, las

Directrices específicamente establecen que los DPO "*no son personalmente responsables en caso de incumplimiento del [GDPR]*"[52].

El incumpliendo de alguna de las normas establecidas en el GDPR será entonces responsabilidad de la organización en la que trabaja el DPO o que lo contrató. No el propio DPO a título personal.

Sin embargo, e independientemente de que, desde el punto de vista del GDPR no hay una sanción específica para el DPO, el DPO tiene en deber de rendir cuentas frente al responsable o encargado de tratamiento de datos para el que trabaja. En este marco, tiene que ser capaz de demostrar que ha trabajado en forma diligente y utilizando todas las medidas a su disposición para cumplir con la tarea que le fue encomendada.

Por otro lado, RECIO[53] sostiene que si bien no hay una responsabilidad personal del DPO por un incumplimiento por parte de la organización en los términos del GDPR, el DPO tiene un rol muy importante a la hora de mitigar los riesgos que pudieran ocurrir sobre los datos objeto de tratamiento. Y así, evitar que esos riesgos se potencien y por supuesto colaborar para que la organización a la que pertenece cumpla y haga cumplir las prescripciones del GDPR.



[52] Grupo de trabajo sobre protección de datos del artículo 29. "*Directrices sobre los delegados de protección de datos (DPD)*". WP 243 rev.01. Adoptadas el 13 de diciembre de 2016 y revisadas por última vez y adoptadas el 5 de abril de 2017. Disponible el 22 de febrero de 2020 en: https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf

[53] Recio, Miguel "Data Protection Officer: The Key Figure to Ensure Data Protection and Accountability", 3 Eur. Data Prot. L. Rev. 114 (2017) Content downloaded/printed from HeinOnline Mon Dec 10 06:00:29 2018)

Distinta es la situación de aquellas organizaciones contratadas por una empresa para actuar como DPO. En ese caso, RUBIÓ[54] sostiene que, cuando el DPO es una organización externa el alcance de su responsabilidad será de dos tipos.

Por un lado, una responsabilidad contractual que le cabe por el servicio para el que fue contratado. Por otro lado, una responsabilidad extracontractual por la forma en que el servicio fue provisto y por los daños generados por tal servicio, por ejemplo, cuando algún titular de un dato sufra un daño como consecuencia de servicio prestado por el DPO externo.

Finalmente, y tal vez lo más importante de todo, hay que destacar que, si bien el GDPR no prevé sanciones penales o administrativas para los DPO, otros países del mundo si las prevén. Las sanciones van desde multas administrativas hasta pena de prisión tal es el caso de Malasia donde la pena de prisión puede ser de hasta los 2 años[55].

HANRATTY[56] en un artículo publicado por la *International Association of Privacy Professionals* hace referencia distintas penas o sanciones aplicadas a los DPO en países ubicados fuera de la Unión Europea. En su artículo, HANRATTY detalla que, por ejemplo, en Hong Kong las multas son de aproximadamente ciento treinta mil dólares estadounidenses y se prevé una pena de hasta cinco años de prisión mientras que en

54 Rubió, Robert 2018. "El Reglamento General de Protección de Datos en el sistema español: el delegado de protección de datos" *Working Papers (Càtedra Jean Monnet de Dret Privat Europeu)* Consultado el 21 de julio de 2019 http://hdl.handle.net/2445/122743

55 Ross David, GDPR and the Role of the Data Protection Officer. Octubre 1, 2018. Disponible el 2 de febrero de 2020 en http://www.rmmagazine.com/2018/10/01/gdpr-and-the-role-of-the-data-protection-officer/

56 Hanratty, Carissa – International Association of Privacy Professionals (2018) "Legal risks to being a DPO" Disponible el 02.02.2020 en https://iapp.org/media/pdf/resource_center/DPO-Liability-Whitepaper-FINAL.pdf

Filipinas será de entre seis meses a siete años de prisión y, en Singapur de uno a tres años de prisión.

En todas esas jurisdicciones y también en el Reino Unido, Irlanda y Canadá, existe también la responsabilidad por daños. En Argentina, por el momento, no existe una pena específica para la figura del DPO sin perjuicio de los remedios generales civiles previstos en la legislación de fondo.

Siendo este tipo de responsabilidades, sobretodo la prisión, de tipo personal será muy importante que cada DPO esté especialmente alerta a la normativa vigente en materia de datos personales en cada una de las jurisdicciones donde la empresa para la que trabaja opera. Por otro lado, es recomendable que los DPO presten especial atención a documentar todas las acciones llevadas a cabo dentro de su empresa para hacer cumplir la normativa de datos personales, no solo del GDPR sino también de la aplicable a cada jurisdicción donde la empresa para la que trabajen opere.

Finalmente, vale destacar también sobre este punto que en enero de 2020 entró en vigencia en California - Estados Unidos, la *California Consumer Privacy Act*[57]. Esta es la primera ley de aquel país que, regula temas de privacidad de datos desde la óptica del GDPR, es decir, desde el paradigma de que los titulares de los datos son las personas y se trata de protegerlos a ellos a la hora de tratar esos datos.

La *California Consumer Privacy Act* no es objeto de este trabajo y no prevé ni la designación de un DPO ni sanciones tan fuertes como las del GDPR. Sin embargo, no

[57] Se puede consultar el texto completo de la ley acá: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121

quería dejar de hacer referencia a esta norma porque es un primer avance hacia nueva regulación sobre estos temas en Estados Unidos y porque podría afectar en el futuro, también las responsabilidades de los DPO.

En este marco, será crucial que se documente cada acción recomendada por el DPO y que, finalmente por una decisión del directorio o de quién tuviera la facultad para tomarla, no se hayan llevado a cabo. La documentación de toda esta información servirá luego como prueba para la defensa en cualquier instancia iniciada contra el DPO.

## V. CONCLUSIONES

Luego de la investigación que realicé para hacer este trabajo, he llegado a las conclusiones que abajo detallo:

- En función de la aplicación extraterritorial del GDPR, gran cantidad de empresas argentinas son potencialmente susceptibles de tener que aplicar sus prescripciones.

- Siguiendo el principio de responsabilidad proactiva, cada empresa argentina deberá analizar su situación particular y determinar si los puntos de contacto que la unen con la Unión Europea son suficientes como para tener que aplicar el GDPR. Ese análisis es recomendable que quede documentado sobre todo en aquellos casos donde exista cierta duda o discusión sobre la aplicación del GDPR.

- Una vez que una empresa argentina defina que le corresponde sujetarse a las normas del GDPR, deberá definir si – además – debe o quiere nombrar un DPO.

- Deberá nombrar obligatoriamente un DPO si (i) su actividad principal consiste en una observación de los titulares de los datos habitual, sistemática y a gran escala; o (ii) si trata categorías especiales de datos (datos sensibles o antecedentes penales a gran escala.

- Las empresas argentinas – siguiendo el principio de responsabilidad proactiva- podrán igualmente nombrar un DPO cuando no entren en ninguna de estas dos categorías. En ese caso, deberán tener especialmente en cuenta si quieren que su DPO sea un DPO en los términos del GDPR o si prefieren nombrar el cargo de otra manera de forma de no tener que cumplir con todas las prescripciones del GDPR respecto de los DPO.

- En caso de nombrar un DPO la empresa argentina deberá tener en cuenta la normativa del GDPR sobre todo respecto de la independencia del DPO para ejercer sus funciones.



- El DPO es mucho más que un auditor interno, es además la persona que hace posible el cumplimiento dentro de la organización a la que pertenece de la normativa sobre protección de datos personales.

- El DPO es el responsable de generar una cultura de protección de datos dentro de la organización a la que pertenece.

- El DPO tendrá diversos desafíos a la hora de ejercer su cargo. Por un lado, deberá logar que desde la organización confíen en el para que pueda realizar correctamente

sus funciones y no le escondan información generando así un cambio cultural. Deberá además señalar aquellos comportamientos dentro de la organización que impidan el cumplimiento de las prescripciones del GDPR debiendo encontrar un equilibrio entre su deber de confidencialidad y lealtad a la empresa en la que trabaja.

- El DPO deberá finalmente tener muy presente sus obligaciones bajo el GDPR y la normativa vigente en materia de datos personales en cada país donde opere la empresa para evitar incurrir en alguno de los supuestos de responsabilidad sancionados por las normas locales.

- Finalmente, es entonces un gran desafío para las empresas argentinas y para los DPO designados por ellas, generar un puesto de trabajo que sea visto no como un policía que impide llevar a cabo ciertos negocios sino más bien como aquella persona que, desde la óptica de la normativa sobre datos personales, puede colaborar para que los proyectos sean exitosos.



## VI. BIBLIOGRAFÍA

AAIP - Aportes sobre la necesidad de una reforma a la Ley de Protección de Datos Personales. Recopilación de los aportes y comentarios recibidos, durante los meses de agosto y septiembre de 2016, en el proceso de reflexión sobre la necesidad de reformar la ley vigente: Disponible el 02 de febrero de 2020 en: https://www.argentina.gob.ar/sites/default/files/documento_aportes_reforma_ley 25326_0.pdf

Altmark, Daniel Ricardo y Molina Quiroga, Eduardo: "Régimen jurídico de los bancos de datos", Editorial Desalma, colección "Informática y Derecho", volumen 6.

Arshad Noor, "Data Protection for Companies," GPSolo 26, no. 2 (March 2009): 40-41

Association of Data Protection Officers of Germany (BvD) e.V. (2018) “Code of Practice for Data Protection Officers” Disponible el 21 de julio de 2019 en https://www.bvdnet.de/wp-content/uploads/2018/04/BvD-Berufsbild_Auflage-4_dt_en.pdf

Basterra, Marcela I. *Obligaciones de los responsables de los bancos de datos. El estándar de calidad de la información*. 2014. La Ley (LA LEY 28/10/2014, 5 • LA LEY 2014-F , 91)

Bazán, Víctor: “La protección de datos personales y el derecho de autodeterminación informativa en perspectiva de Derecho comparado”. LLGran Cuyo2005 (junio), 453.

Beckerman, Jorge: "Banco de Datos y responsabilidad objetiva", Congreso Internacional de Informática y Derecho, AABA-ADIJ, Bs.As., octubre 1990, 390.

Bermúdez Durana, Fernando, "El principio de accountability en el anteproyecto de protección de datos de Argentina", Revista Latinoamericana de Protección de Datos nro. 4, CDYT, 2018, p. 89.

Bianchi, Alberto: “Hábeas data y derecho a la privacidad”. El Derecho, 161-866.

Binns, Reuben, Data Protection Impact Assessments: A Meta-Regulatory Approach (December 13, 2016). International Data Privacy Law, Vol. 7(1), p. 22-35, 2017. Disponible el 06 de marzo de 2020 en https://ssrn.com/abstract=2964242

Cabrera, Romina Florencia: Protección de datos, globalización y nuevas tecnologías. Sup. Act. 29/07/2014, 29/07/2014, 2. AR/DOC/2572/2014.

Centre for information policy leadership (2016) Ensuring the Effectiveness and Strategic Roleof the Data Protection Officer under the General Data Protection Regulation. Disponible el 21 de julio de 2019 en https://iapp.org/media/pdf/resource_center/cipl_gdpr_dpo_17_nov_2016.pdf

Cifuentes (h.), Santos E.: “La protección de datos personales y el Internet”. LA LEY 10/10/2007, 10/10/2007, 1 - LA LEY2007-F, 761 - Enfoques 2007-11 (noviembre), 10/10/2007, 82.

Cifuentes, Santos: “Derecho personalísimo a los datos personales”. LA LEY 1997-E, 1323.

Ciruel, Alicia I.: “La protección de los datos personales. Análisis a la luz del derecho comparado”. DJ2004-4, 229.

D'Hulst, Thibaut y Kengen, Lily, Data protection compliance strategy, Global Guide to data protection, Practical law, 2018. Disponible el 22 de enero de 2019 en *https://uk.practicallaw.thomsonreuters.com/w-0116784?comp=pluk&transitionType=Default&contextData=(sc.Default)*

Durrieu, Nicolás, “El Oficial de Cumplimiento: su responsabilidad penal y administrativa”, 2915. Disponible en Abogados.com.ar el 12.03.2020 en https://www.abogados.com.ar/el-oficial-de-cumplimiento-su-responsabilidad-penal-y-administrativa/17120

Hanratty, Carissa – International Association of Privacy Professionals (2018) “Legal risks to being a DPO” Disponible el 02 de febrero de 2020 en https://iapp.org/media/pdf/resource_center/DPO-Liability-WhitepaperFINAL.pdf

Hunton & Williams LLP – Centre for Information Policy Leadership (2016) “Ensuring the Effectiveness and Strategic Role of the Data Protection Officer under the General Data Protection Regulation” - GDPR Project DPO Paper, November 17, 2016

Díaz Molina, Iván: "El Derecho de Privacy en el Common Law y en el Derecho Civil (estudio comparativo)", en Boletín de la Facultad de Derecho y Ciencias Sociales de la Universidad Nacional de Córdoba, año XXVII.

Faliero, Johanna Caterina *El futuro de la regulación en protección de datos personales en la argentina.* 2018. Suplemento Especial LegalTech Thomson Reuters

Frene, Lisandro, *Reglamento general de protección de datos de la unión europea. Extraterritorialidad e impacto en argentina*. 2018. La Ley (LA LEY 2018-E, 1275 - Cita Online: AR/DOC/1764/2018)

Hielke Hijmans, "How to Enforce the GDPR in a Strategic, Consistent and Ethical Manner," European Data Protection Law Review (EDPL) 4, no. 1 (2018): 80-84 Bluebook

Hintze, Mike. "Viewing the GDPR through a De-Identification Lens: A Tool for Compliance, Clarification, and Consistency." *International Data Privacy Law* 8, no. 1 (02, 2018): Disponible el 10 de diciembre de 2018 en https://search-proquest-com.eza.udesa.edu.ar/docview/2056424778?accountid=28034

de Hert, Paul M Czerniawski Michal (2016); Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context, *International Data Privacy Law*, Volume 6, Issue 3, 1 August 2016, Pages 230–243, https://doi.org/10.1093/idpl/ipw008

Goswan, Suparna "GDPR Compliance: Should CISO Serve as DPO? Sorting Out the Role of the Data Protection Officer" Disponible el 06 de marzo de 2020 en https://www.bankinfosecurity.com/authors/suparna-goswami-i-1945

Grupo de trabajo sobre protección de datos del artículo 29. "*Directrices sobre los delegados de protección de datos (DPD)*". WP 243 rev.01. Adoptadas el 13 de diciembre de 2016 y revisadas por última vez y adoptadas el 5 de abril de 2017. Disponible el 22 de febrero de 2020 en: https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf

Ibrahimi, Silvia; Dervishi, Eglantina, Ibrahimi, Ervin (2018) "Cyberdeviance and the Role of Data Privacy Officer's Sustainable Structures in its Prevention". Disponible el 21 de junio de 2019 en https://doi.org/10.32591/coas.ojpr.0202.02061i

Kuner, C., Cate, F., Lynskey, O., Millard, C., Loideain, N. N., & Svantesson, D. (2018). An unstoppable force and an immoveable object? EU data protection law and national security. *International Data Privacy Law, 8*(1), 1-3. doi:http://dx.doi.org.eza.udesa.edu.ar/10.1093/idpl/ipy003

Kuner, Christopher 'The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law' Bloomberg BNA Privacy and Security Law Report (6 February 2012) 1–15. (disponible el 12 de

marzo de 2019 en http://robertgrzeszczak.bio.wpia.uw.edu.pl/files/2012/12/Kuner_A-CopernicanRevolution-in-European-Data-Protection-Law.pdf)

Lambert, Paul. (2017). The Data Protection Officer. New York: Auerbach Publications, Disponible el 20 de febrero de 2020 en https://doi.org/10.1201/9781315396743

Layton, Roslyn, "How the GDPR Compares to Best Practices for Privacy, Accountability and Trust" disponible el 22 de enero de 2019 en http://dx.doi.org/10.2139/ssrn.2944358.

Masciotra, Mario: "El controvertido ámbito de aplicación de la ley de protección de datos personales". LA LEY 29/02/2008, 29/02/2008, 3 - LA LEY2008-B, 166.

Milanes, Valeria. Algoritmos y discriminación en el marco de la ley de protección de datos personales. 2018. La Ley (SJA 06/06/2018, 34 • JA 2018-II, 1342)

Minero Alejandre, Gemma. Presente y futuro de la protección de datos personales. Análisis normativo y jurisprudencial desde una perspectiva nacional y europea. Anuario jurídico y económico escurialense, 2017, Issue 50, pp.13-58. Fundación Dialnet

Palazzi, Pablo A. *Compliance y protección de datos personales.* 2018 Suplemento Especial Compliance Thompson Reuters

Palazzi, Pablo A. *Transferencia internacional de datos personales. Nueva regulación de la dirección nacional de protección de datos personales*. 2018. La Ley (LA LEY 15/02/2017, 1 LA LEY 2017-A, 1039)

Palazzi, Pablo A. *"Ámbito de aplicación de la ley de protección de datos personales." Suplemento del 21-8-2002. JURISPRUDENCIA ARGENTINA, Buenos Aires, Jurisprudencia Argentina, Volumen: 2002-III, 26 - 33.*

Platt, Gordon (2016) Data Protection Officers In Demand In Europe Global Finance*; Jul/Aug 2016; 30, 7; ABI/INFORM Collection pg. 81*

Poullet, Yves, coord.; PÉREZ ASINARI, María Verónica, coord.; PALAZZI, Pablo A., coord.: *"Derecho a la intimidad y a la protección de datos personales"*. Editorial Heliasta. Buenos Aires, 2009, 1a ed., ISBN 978-950-885-110-9, 2009, 251.

Recio Miguel, "Data Protection Officer: The Key Figure to Ensure Data Protection and Accountability," European Data Protection Law Review (EDPL) 3, no. 1 (2017): 114-118.

Rubió, Robert 2018. "El Reglamento General de Protección de Datos en el sistema español: el delegado de protección de datos" *Working Papers (Càtedra Jean Monnet de Dret Privat Europeu)* Consultado el 21 de julio de 2019 http://hdl.handle.net/2445/122743

Travieso, Juan Antonio. La protección de datos personales: problemas y sistemas. 2014. La Ley (LA LEY 08/04/2014 ,1 • LA LEY 2014-B , 808)

Travieso, Juan Antonio. Régimen jurídico de los datos personales. 2014. Buenos Aires. La Ley.

Ross David, GDPR and the Role of the Data Protection Officer. October 1, 2018. Disponible el 2 de febrero de 2020 en http://www.rmmagazine.com/2018/10/01/gdpr-and-the-role-of-the-data-protection-officer/

Suparna Goswam. GDPR Compliance: Should CISO Serve as DPO? Sorting Out the Role of the Data Protection Officer. Disponible el 20.02.2020 en https://www.bankinfosecurity.com/gdpr-compliance-should-ciso-serve-as-dpo-a-13722

Vila, Carolina Abdelnabe. 2019. "Argentina se adapta a la normativa europea, mientras espera la sanción de la nueva Ley de Protección de Datos Personales." *Abogados.com.ar*. Disponible el 03.03.2020 en https://www.abogados.com.ar/argentina-se-adapta-a-la-normativa-europea-mientras-espera-la-sancion-de-la-nueva-ley-de-proteccion-de-datos-personales/22921 .