Universidad Internacional de La Rioja

Facultad de Derecho

Máster Universitario en Protección de Datos

EL MODELO DE ACCOUNTABILITY EN LA NORMATIVA DE PROTECCIÓN DE DATOS PERSONALES

Trabajo fin de estudio presentado por:	Valeria Alejandra Ordóñez Segarra
Tipo de trabajo:	Trabajo fin de Master
Director/a:	Santiago Bermell Girona
Fecha:	10/07/2024

Resumen

A título ilustrativo, es oportuno indicar que el principio de responsabilidad proactiva también llamada accountability en inglés, es fundamental en el ámbito de la protección de datos. El Reglamento General de Protección de Datos determina la aplicación demostrable de la protección de datos que permite acreditar el cumplimiento de las obligaciones establecidas en la normativa. En este contexto, es necesario que el responsable del tratamiento implemente medidas organizativas y técnicas adecuadas para asegurar y demostrar que el procesamiento de datos personales cumple con los requisitos establecidos en el Reglamento.

En el presente trabajo, se abordará los diferentes desafíos que pueden tener las organizaciones en implementar medidas proactivas, lo que implica una mayor responsabilidad y esfuerzo en la gestión de la privacidad y seguridad de los datos. En efecto, se pretende analizar la actividad de tratamiento, sintetizar su significado, obligaciones, alcance, fomentar una cultura de cumplimiento, dar un paso crucial hacia una gestión responsable de la información.

Palabras clave: Responsabilidad proactiva, Privacidad desde el diseño, Privacidad por defecto, Delegado de protección de datos, Gestión del riesgo

(De 3 a 5 palabras)

Abstract

By way of illustration, it is appropriate to indicate that the principle of proactive responsibility, also called accountability in English, is fundamental in the field of data protection. The General Data Protection Regulation determines the demonstrable application of data protection that allows the compliance with the obligations established in the regulations to be accredited. In this context, it is necessary for the data controller to implement appropriate organizational and technical measures to ensure and demonstrate that the processing of personal data complies with the requirements set out in the Regulation.

In this work, the different challenges that organizations may face in implementing proactive measures will be addressed, which implies greater responsibility and effort in the management of data privacy and security. In fact, the intention is to analyze the processing activity, synthesize its meaning, obligations, scope, foster a culture of compliance, and take a crucial step towards responsible information management.

Keywords: Accountability, Privacy by design, Privacy by default, Data Protection Officer, Risk management

Índice de contenidos NO ABREVIATURAS

1. Introducción

La normativa europea sobre protección de datos tuvo su inicio en la Directiva 95/46/CE [1]emitida el 24 de octubre de 1995. Sin embargo, esta fue reemplazada posteriormente por el Reglamento (UE) 2016/679[2], el cual entró en vigor el 24 de mayo del 2016, aplicándose desde el 25 de mayo de 2018. El nuevo reglamento propone un enfoque basado en el riesgo, que incluye la necesidad de documentar la realización de análisis de riesgos y evaluaciones de impacto entre otros. Esto, lógicamente, podría aumentar los costos de desarrollo. (MORTIZ, GIBELLO 2021, p. 1).

Sobre la base de lo expuesto, la orientación basada en el riesgo (risk-based approach)[3] implica la creación de un marco normativo que se adapta a los riesgos específicos de una actividad en particular, en lugar de seguir una lógica binaria de cumplimiento o incumplimiento. Este enfoque se conoce comúnmente como cumplimiento normativo o *compliance*[4]. (BARRIO 2023).

Ahora bien, (MORTIZ,GIBELLO 2021,p.3), sostiene que si trasladamos esta cuestión al ámbito del derecho a la protección de datos personales, se hace necesario que el responsable del tratamiento de datos, en el caso de presentar un riesgo elevado para la privacidad de las personas, deba destinar una mayor cantidad de recursos para el cumplimiento de las regulaciones. Esto conlleva la adopción de medidas de seguridad más robustas, protección de datos desde el diseño y por defecto y el nombramiento de un delegado de Protección de

[1] Directiva 95/46/CE del parlamento europeo y del consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
[2] REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)
[3] risk-based approach consiste en la promulgación de un marco normativo en el que los deberes y obligaciones se escalonan y adaptan a los riesgos concretos derivados de una actividad específica. BARRIO,M.<< *El cumplimiento basado en el riesgo o risk-based compliance, pieza cardinal del nuevo Derecho digital europeo*.Real Instituto el Cano Royal Institute.2023. disponible en: https://media.realinstitutoelcano.org/wp-content/uploads/2023/04/el-cumplimiento-basado-en-el-riesgo-o-risk-based-compliance-pieza-cardinal-del-nuevo-derecho-digital-europeo-real-instituto-elcano.pdf
[4]compliance*[4]:* Prevención de riesgos corporativos: en inglés, compliance programme) y un responsable de cumplimiento normativo o Compliance Officer. BARRIO,M.<< *El cumplimiento basado en el riesgo o risk-based compliance, pieza cardinal del nuevo Derecho digital europeo*.Real Instituto el Cano Royal Institute.2023. disponible en: https://media.realinstitutoelcano.org/wp-content/uploads/2023/04/el-cumplimiento-basado-en-el-riesgo-o-risk-based-compliance-pieza-cardinal-del-nuevo-derecho-digital-europeo-real-instituto-elcano.pdf

Datos en adelante (DPO) y la realización de una evaluación de impacto correspondiente, entre otras.

Atendiendo a estas consideraciones, el Reglamento (UE) 2016/679, de 27 de abril de 2016 en adelante, (RGPD) no ofrece una definición clara acerca del concepto de riesgo, aunque los requisitos impuestos a quienes manejan datos personales se establecen en función de un enfoque basado en el riesgo inherente al tratamiento de dichos datos. (MORTIZ, GIBELLO 2021,p.1).

En este sentido, el artículo 5.2 del Reglamento establece que el responsable del tratamiento de datos es garante de cumplir con todos los principios establecidos por la regulación, y además debe ser capaz de demostrar dicho cumplimiento. La novedad del principio de rendición de cuentas o accountability se manifiesta a través de la incentivación de una actitud más proactiva por parte de los responsables, que no solo buscan cumplir con los requisitos de protección de datos, sino también demostrar su cumplimiento mediante elementos concretos. Con este enfoque, se busca pasar de un abordaje reactivo a uno más proactivo. En consonancia con lo anterior, el Reglamento incorpora una serie de medidas destinadas a ayudar al responsable a cumplir con el principio de accountability. Estas medidas incluyen la privacidad desde el diseño y por defecto, el nombramiento de un Delegado de Protección de Datos (DPD), el enfoque de en los riesgos en materia de seguridad, entre otras. En conjunto, estas disposiciones buscan establecer una nueva filosofía de respeto por las normativas de protección de datos, involucrando a todos los elementos y actores que se encuentran implicados en el tratamiento de datos personales dentro de una organización. En consecuencia, se trata de fomentar una cultura de protección de datos. (MURGA, FERNANDEZ Y ESPEJO 2018,P.48).

En esta misma línea, la Agencia Española de Protección de Datos, en adelante (AEPD), en su guía de protección de datos por defecto, puntualiza que para la adopción de cualquier medida de responsabilidad proactiva implica desglosar el tratamiento en sus distintas fases, identificar las operaciones de tratamiento realizadas en cada una de ellas, comprender las particularidades de cada fase y optimizarlas, especialmente en lo relacionado con la protección de datos, lo cual forma parte de la estrategia para una aplicación efectiva de las medidas de responsabilidad proactiva (AEPD. Guía de Protección de Datos por Defecto).

En tal virtud, la contribución de este TFM es facilitar la comprensión del principio de responsabilidad proactiva, mediante un trabajo de síntesis y jurídico que abordara los puntos más relevantes para su aplicación y cumplimiento.

1.1. Justificación del tema elegido

Es oportuno examinar en detalle el marco normativo europeo actual en materia de privacidad, liderado por el RGPD. Este marco presenta numerosas innovaciones, tales como la responsabilidad proactiva, una mayor importancia de la privacidad desde el diseño y por defecto, y la creación de la figura del delegado de protección de datos. Todas estas innovaciones han revolucionado la regulación de la privacidad (DOMINGUEZ 2022).

Como seguimiento a esta actividad, el uso de big data[5] para el procesamiento de datos personales puede ser impredecible porque a menudo no se sabe para qué fines se utilizará esa información o qué información nueva se creará a partir de ella. Por lo tanto, es vital que las organizaciones se centren en el principio de Responsabilidad Proactiva para abordar las dificultades relacionadas con la protección de datos personales. Las decisiones basadas en información algorítmica pueden tener un impacto social significativo; por lo tanto, deben diseñarse e implementarse de manera responsable. Esto incluye la obligación de informar, explicar y justificar decisiones específicas, así como mitigar los impactos negativos y potenciales daños (HUESCA 2019).

En este sentido, es importante señalar que la Evaluación de Impacto se define como una herramienta para identificar los posibles riesgos que el tratamiento de información personal puede generar en sistemas, procesos, infraestructura y actividades del personal en una organización. Esta identificación proactiva permite la gestión adecuada de dichos riesgos para evitar su ocurrencia en las organizaciones (COTE 2020).

[5] La expresión Big Data hace referencia a las herramientas, procesos y procedimientos que posibilitan a una organización la creación, manipulación y gestión de extensos conjuntos de datos y sistemas de almacenamiento.

De lo anteriomente expuesto, en vista de los avances tecnológicos actuales, es crucial tomar en cuenta el principio de responsabilidad proactiva y las medidas que deben ser implementadas por el responsable de tratamiento, moviéndose de un enfoque reactivo a uno más preventivo. Además, se ha reconocido la autoridad de control como la encargada de garantizar el cumplimiento de la normativa (TRUJILLO, FERNANDEZ y CABRERA 2018. p.143).

1.2. Problema y finalidad del trabajo

En relevante determinar que el principio de accountability es un concepto amplio que bien podría identificarse con la definición de «concepto jurídico indeterminado» (ESTEPA 2022, p.10). Uno de los componentes mas importantes es la capacidad para demostrar la integridad en el diseño y manejo del tratamiento de datos; mediante el cual, se puede dilucidar con la valoración realizada en un juicio a hoc por una Autoridad de control independiente o un Órgano judicial especializado. Dentro de esta perspectiva; diferentes autoridades de supervisión o jurisdicciones pueden interpretar el principio de manera diversa, lo que puede generar inconsistencias en su aplicación (ESTEPA 2022).

Como se puede inferir, el artículo 25 y el Considerando 74 del RGPD establecen claramente que la gestión del tratamiento de datos debe tener en cuenta la naturaleza, el ámbito, el contexto y los fines del mismo, así como el riesgo que este pueda tener para los derechos y libertades de las personas. También se requiere que las medidas tomadas sean revisadas y adaptadas en caso de que cambien las circunstancias. Este es un concepto dinámico que surge de la necesidad de lograr un nivel de eficacia y transparencia en la actividad pública y privada, garantizando siempre el respeto al Ordenamiento jurídico y unos estándares mínimos de calidad. En definitiva, la responsabilidad proactiva se configura como un instrumento para lograr estos objetivos y puede ser ampliada y profundizada en función del grado de desarrollo tecnológico y social (ESTEPA 2022).

Partiendo de los supuestos anteriores, es necesario identificar y abordar la existencia de una dificultad relación entre la seguridad jurídica y los aspectos tecnológicos desde una perspectiva más concreta, considerando la singularidad de los servicios tecnológicos que se prestan en la actualidad. Esto implica considerar tanto la situación legal de los ciudadanos como el control efectivo que los responsables del tratamiento de datos tienen sobre la configuración y funcionamiento de aplicaciones y sistemas de información. Es crucial evitar

una perspectiva restringida que se centre únicamente en las consecuencias legales del incumplimiento de las garantías tecnológicas de privacidad para los ciudadanos. Se deben proporcionar medidas de protección adecuadas para cualquier uso de la informática que viole los derechos de las personas, independientemente de si afecta o no la información relacionada con su identidad física, ya sea identificada o simplemente identificable (VALERO 2007).

1.3. Objetivos

Esta investigación analiza el concepto de responsabilidad proactiva o accountability en el marco de la nueva legislación referente a la protección de datos personales. En efecto, surge la necesidad de delimitar el alcance del principio y, su interpretación. Analizar la actitud proactiva que la misma AEPD ha determinado «no incumplir ya no será suficiente». El objetivo de la investigación radica en examinar el cumplimiento lo que permitiría asegurar el necesario respeto a los derechos de los particulares a la vez que se facilite el continuo aumento del flujo de datos que se comparte entre las empresas de manera adecuada. En este orden de ideas, concretar y precisar el concepto jurídico indeterminado.

Con relación a estas implicaciones, nos enfocaremos en dos objetivos específicos:

El primer objetivo es determinar el centro de la responsabilidad para las personas jurídicas, lo cual implicaría demostrar la protección efectiva que permita verificar el cumplimiento de las obligaciones establecidas en la normativa, centrándose en asuntos de seguridad, privacidad desde el diseño y por defecto, y la figura del delegado de protección de datos.

El segundo objetivo es crear un conjunto de directrices en analogía con el tratamiento masivo de datos personales que vaya más allá de las medidas legales, organizativas y técnicas existentes. Este conjunto de directrices establecerá límites adicionales sobre lo que debe hacerse o no, lo que contribuirá al cumplimiento correcto del Reglamento General de Protección de Datos (RGPD).

2. Marco teórico y desarrollo

2.1. Contexto global del principio de responsabilidad proactiva

Como se ha expresado previamente, la utilización indebida de información personal en la era digital y de la información puede generar graves perjuicios a la privacidad, lo cual demanda que cualquier uso estructurado de datos personales cuente con las apropiadas garantias para las personas afectadas. El desafío se ha vuelto más complejo debido al gran flujo de información entre corporaciones, entidades públicas y particulares (ESTEPA 2022). En este contexto, en 1980, la Organización para la Cooperación y Desarrollo Económico, en adelante (OCDE)[6] introdujo el principio de responsabilidad proactiva o accountabiliy en los Códigos de Conducta o Guías de Protección de la Privacidad y Flujo Transfronterizo de Datos.(CLUB LEGAL ASESORES INTERNACIONALES, 2022). La promulgación del Convenio 108 por el Consejo de Europa en 1981 marcó un hito al establecer pautas para asegurar la protección de los derechos y libertades esenciales de los individuos en los Estados miembros. En territorio español, la primera normativa que reguló el procesamiento de archivos de datos fue la Ley Orgánica de Regulación del Tratamiento Automatizado de Datos (LORTAD), número 5/1992 del 29 de octubre. Esta ley concedió a las entidades gubernamentales el poder de controlar, supervisar y penalizar para asegurar una gestión adecuada de las operaciones, abarcando sectores tanto públicos como privados. Posteriormente, en el año 2010, el Grupo de Trabajo del artículo 29 en adelante (GT29)[7], un órgano consultivo e independiente de la Unión Europea especializado en privacidad y protección de datos, emitió un informe recomendando la adopción del principio de responsabilidad proactiva dentro de la legislación de protección de datos. Esto significaba que los responsables del procesamiento de datos personales tenían la obligación de probar ante las autoridades pertinentes que habían tomado medidas efectivas y apropiadas para salvaguardar los derechos de protección de datos de los individuos (ESTEPA 2022). La introducción del principio de responsabilidad proactiva se hizo efectiva a través del

[6] La Organización para la Cooperación y el Desarrollo Económicos (OCDE) es un actor central en la cooperación internacional; nuestros miembros colaboran con otros países y organizaciones alrededor del mundo para abordar los desafíos actuales en políticas públicas.
[7] El Grupo de Trabajo del artículo 29 se constituyó en el año 1996 como consecuencia de la entrada en vigor de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de datos de las personas físicas y la libre circulación de estos datos.

RGPD, es obligatorio en todos sus aspectos y tiene una aplicación directa y preferente en cada uno de los Estados miembros, revocando la Directiva 95/46/CE. Se concedió un amplio plazo de "vacatio legis" para permitir que los destinatarios tomaran las medidas necesarias para cumplir adecuadamente con las disposiciones establecidas en el reglamento (ESTEPA 2022).

Es así, que el RGPD y la Directiva 95/46/CE comparten objetivos en común, de garantizar que el tratamiento de datos personales respete los derechos fundamentales y permita la libre circulación de los datos entre los Estados miembros (RODRIGUEZ 2019).

Atendiendo a estas consideraciones, el RGPD, en el Considerando 1, determina que el derecho a la protección de datos personales es un derecho fundamental. En este sentido, este derecho está recogido en la Carta de los Derechos Fundamentales de la Unión Europea[8] y en el Tratado de Funcionamiento de la Unión Europea[9] (TFUE), y tiene como finalidad proteger los datos personales de cualquier individuo. Ahora bien, de cara a cumplir con el principio de responsabilidad proactiva, el RGPD establece una serie de medidas obligatorias para que el responsable del tratamiento de datos (y en algunas situaciones, el encargado) pueda cumplir con el principio de responsabilidad proactiva y demostrar el cumplimiento normativo. Estas medidas incluyen aspectos como la figura del Delegado de Protección de Datos (DPO), medidas de protección de datos desde el diseño y por defecto, seguridad de los tratamientos de datos, registro de actividades de tratamiento, consulta previa, entre otras.

Sobre la base de las ideas expuestas, en la nueva regulación, todas las organizaciones tienen la responsabilidad de llevar a cabo un análisis de riesgos de sus procesamientos de datos. En caso de que este análisis muestre un riesgo elevado, se requerirá una Evaluación de Impacto, y la adopción de medidas necesarias para cumplir con las exigencias del Reglamento Europeo y de las normas internas sobre protección de datos. Estas medidas de seguridad y control se establecen para proteger los derechos y libertades de las personas. El propósito es lograr una protección más eficaz del derecho fundamental a la protección de datos y, simultáneamente, fomentar políticas preventivas entre las organizaciones para evitar costosas

[8] Artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea
[9] De acuerdo con el Tratado de Maastricht, el Tratado de Funcionamiento de la Unión Europea (TFUE), que es una continuación del Tratado de Lisboa, se basa en el Tratado constitutivo de la Comunidad Europea (TCE o Tratado CE).

reestructuraciones de los sistemas después de haber sido creados, así como posibles daños a la reputación e imagen por un tratamiento indebido de los datos personales (SOLER 2020).

El segundo elemento es el principio de protección desde el diseño y por defecto, que tiene como objetivo primordial la prevención de posibles riesgos. Se podría decir que la mejor medida consiste en prevenir cualquier eventualidad. En el año 2010, los Comisionados de Protección de Datos y Privacidad aprobaron la "Resolución sobre la privacidad por diseño"[10] (Agencia Española de Protección de Datos 2019). Se basaron en los siguientes principios: <<Proactivo, no reactivo>>; <<preventivo, no correctivo>>. Por lo antes expuesto, es esencial que cualquier sistema, proceso o infraestructura que maneje datos personales sea construido y diseñado desde el inicio. Esto implica la identificación y reducción de riesgos potenciales a los derechos y libertades de las personas para prevenir perjuicios. Por ende, la regulación correspondiente exige que el responsable del tratamiento de datos implemente medidas técnicas y organizativas apropiadas. Estas medidas deben garantizar que únicamente los datos personales imprescindibles sean procesados para cada propósito específico y que, por omisión, dichos datos no sean accesibles a un número ilimitado de personas sin el consentimiento explícito del titular de los datos (WILKINS 2020).

El tercer elemento clave, y no menos importante, es el Delegado de Protección de Datos (DPD), conocido como Data Protection Officer (DPO) en inglés. En el artículo 4 del RGPD, que trata sobre definiciones, se mencionan claramente conceptos como el responsable y el encargado del tratamiento, pero no se incluye una definición explícita del DPO. A primera vista, esto puede ser confuso debido a que el DPO es una de las grandes novedades del Reglamento y se esperaría que su definición estuviera claramente establecida. Sin embargo, una vez que se examinan los artículos 37, 38 y 39 del RGPD que se refieren al Delegado de Protección de Datos, se constata que la falta de dicha definición es una decisión intencional para evitar limitar quiénes pueden desempeñar el cargo. De cualquier modo, a pesar de que no se restrinja quiénes pueden ser DPO, esto no significa que cualquier persona pueda ocupar

[10] En la década de los años 90 y fue presentado en la trigésima primera (31ª) Conferencia Internacional de Comisionados de Protección de Datos y Privacidad del año 2009 bajo el título "Privacy by Design: The Definitive Workshop" siendo posteriormente aceptado internacionalmente en la trigésima segunda (32ª) Conferencia Internacional de Comisionados de Protección de Datos y Privacidad, celebrada en Jerusalén en el año 2010, con la aprobación de la "Resolución sobre la Privacidad por Diseño".

el cargo. El artículo 37.5 del Reglamento establece el perfil que debe tener una persona que ocupe el cargo de DPO y sus cualidades profesionales, incluyendo conocimientos especializados en el ámbito del Derecho y de la protección de datos, y capacidad para desempeñar las funciones indicadas en el artículo 39. El considerando 97 también indica que los conocimientos y aptitudes requeridos deben estar en línea con las operaciones de tratamiento de datos específicas de cada organización, y no pueden basarse en criterios generales. Por tanto, el perfil del DPO debe adaptarse a las características del tratamiento de datos específico de cada organización (GUILLEN 2017).

2.2. Eficacia del principio de responsabilidad proactiva en la protección de datos personales

Para abordar este tema, es necesario conceptualizar en primer orden, lo que es un principio. En palabras de Robert Alexy « Los principio son normas que ordenan que se realice algo en la mayor medida posible, en relación con las posibilidades juridicas y fácticas (mandatos de optimización)[11] (ZAMIR 2011). En efecto, una vez delimitado el concepto de lo que es un principio, en cuanto a la protección de datos se refiere, es un principio fundamental que debe dirigir la conducta del responsable del tratamiento. Es necesario actuar de conformidad con la Ley y poder demotrar el cumplimiento de todas las obligaciones legales.

En este contexto, se podría argumentar que el principio de responsabilidad proactiva no es una idea moderna, ya que la (OCDE) estableció directrices sobre privacidad en 1980 que incluían este principio. El (GT29) señala que este principio fue explícitamente reconocido en dichas directrices y que su contenido establecía que « Todo responsable de datos debería ser responsable de cumplir con las medidas que hagan efectivos los principios materiales expuestos» [...] [12] (GT29.WP173.p.7). Sin embargo, a pesar de que el principio de responsabilidad proactiva no es nuevo, ha sido ignorado por los responsables del tratamiento de datos que no lo aplican de manera permanente. Esto se debe a que éstos se centran

[11] Para Alexy, los principios son mandatos de optimización, y su rasgo definitorio es que pueden cumplirse en diferente grado. Dicho de otro modo, a diferencia de las reglas (normas) , los principios no contienen mandatos definitivos, sino prima facie.

[12] Véase: Dictamen 2/2006 del Grupo de trabajo 29 sobre el respeto de la privacidad en relación con la prestación de servicios de cribado de correo electrónico.

únicamente en cumplir con las leyes locales que rigen en el país donde desarrollan su actividad y no en aplicar medidas adicionales de manera proactiva (SANTAMARIA 2020). De la misma forma, buscan solo el beneficio empresarial y alegan que no se va a poder cumplir con la privacidad. En efecto, es categórico determinar que es un principio básico en materia de protección de datos. Ahora bien, de lo expuesto, cabe plantear la siguiente cuestión: ¿por qué las normas relacionadas con la protección de datos, en ocasiones no son eficaces? La razón radica en que las entidades no garantizan una auténtica protección de los datos personales al interior de sus organizaciones y no es una cuestión personal o un juicio de valor, el GT29 afirma lo mismo. Dicho grupo ofrece varias observaciones valiosas para entender la cuestión actual sobre la responsabilidad como factor clave para una aplicación efectiva de los principios relacionados con la protección de datos personales. Estas observaciones, incluyen que las tecnologías de la información y las comunicaciones han creado un entorno de « diluvio de datos». Esto implica que los datos personales se transfieren a través del mundo constantemente, lo que hace que los responsables de su tratamiento necesiten tener en su disposición mecanismos eficaces para garantizar la protección adecuada de estos datos personales. De la misma manera, enfatiza que los datos personales tienen un valor creciente en aspectos sociales, políticos y económicos. De hecho, se han vuelto tan importantes que algunos individuos los intercambian por acceso a contenido. Por tanto, los datos personales se han convertido en un bien de valor, lo cual resalta la necesidad de establecer medidas de protección efectivas. Tanto en el sector público como en el privado, la situación actual puede provocar filtraciones de información con consecuencias negativas considerables. Por ello, es crucial que los responsables del tratamiento de datos mantengan una buena reputación y la confianza de las personas (GT29.173.p.5).

¿Por qué es importante la aplicación del principio de responsabilidad proactiva en cualquier tipo de institución? Porque cumplir con la normativa de protección de datos no solo evita la posibilidad de sanciones, sino que también mejora la imagen y reputación de la organización, genera confianza en los usuarios y clientes, y reduce los riesgos y costos económicos. Si todas las instituciones, tanto públicas como privadas, entienden esto, se mejorará la protección de los datos personales independientemente de las leyes que deban cumplir, lo ideal seria fomentar la cultura de la privacidad. En resumen, el responsable del tratamiento de datos

debe actuar en dos capas: la capa "de mínimos"[13], cumpliendo con la legislación en protección de datos de carácter personal aplicable; y la capa "de máximos"[14], implementando sistemas opcionales de responsabilidad que brinden garantías más estrictas que las impuestas por la ley (SANTAMARIA 2020).

Partiendo de los supuestos anteriores, el GT29 hace referencia a las normas Técnicas Internacionales adoptadas en Madrid [15] por las Autoridades de protección de datos, incluyendo la disposición del artículo 22 que establece medidas proactivas que motivaron al RGPD siete años después a hablar específicamente del principio de responsabilidad proactiva. Además, se presenta una lista detallada de medidas que podrían ser beneficiosas para implementar el principio de responsabilidad proactiva, incluyendo la implementación de procedimientos de gobernanza, nombramiento de "funcionarios" de protección de datos, programas de formación, educación y sensibilización, auditorías transparentes, adaptación de sistemas de información y evaluaciones de impacto, adopción de códigos de prácticas y planes de respuesta ante posibles vulneraciones de la normativa de protección de datos personales (GT29 173 .p. 12).

Es importante destacar que la cuestión de las sanciones en relación con la protección de datos es un matiz relevante. ¿Cumplir con el principio de responsabilidad proactiva exime a los responsables del tratamiento de sanciones por incumplimiento de la normativa en protección de datos? La respuesta es no. Aunque un responsable del tratamiento de datos personales desarrolle una buena gobernanza en este tema, esto no significa que esté protegido de posibles sanciones en caso de incumplimiento de la normativa. Sin embargo, las autoridades reguladoras pueden considerar la aplicación de sanciones menos graves si consideran que el responsable está actuando de manera más rigurosa y respetando la legislación de manera adecuada. Como se mencionó anteriormente, es importante recordar que el principio de

[13] Capa de Mínimos", donde el responsable se enfoca en cumplir con la normativa mínima requerida en la materia. Véase mas: https://dialnet.unirioja.es/servlet/articulo?codigo=8023446

[14] Capa de máximos: donde el responsable asume una postura proactiva y establece sistemas internos de responsabilidad facultativos adicionales a los requeridos por la legislación, proporcionando garantías más rigurosas. Véase más: : https://dialnet.unirioja.es/servlet/articulo?codigo=8023446

[15] Se trata de una propuesta conjunta para la creación de estándares internacionales para la protección de la privacidad en relación con el tratamiento de datos personales. Esta propuesta ha sido bien recibida por la 31ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, celebrada en Madrid el 5 de noviembre de 2009. Para su consulta a través del siguiente enlace: https://edps.europa.eu/sites/edp/files/publication/09-11-05_madrid_int_standards_es.pdf

responsabilidad proactiva, al menos en el ámbito europeo, se encuentra dentro del marco legal más que en el ámbito ético(SANTAMARIA 2020).

2.3. La gestión del riesgo como elemento concluyente en aplicación del principio de responsabilidad proactiva

En esta sección, nos enfocaremos en la seguridad como un elemento integrante del modelo preventivo de la accountability, con especial atención a la gestión de riesgos. En la actualidad, por lo que respecta a la normativa en materia de protección de datos personales, este derecho a la seguridad se materializa con carácter fundamental, en el artículo 32 [16] RGPD**;** que, partiendo de la previsión contemplada en el precitado artículo 5.1.f[17] del RGPD.

Como se puede inferir, la responsabilidad en caso de vulnerarse el artículo 32 íbidem, recaerá directamente sobre el responsable del tratamiento o sobre el encargado del tratamiento. De este modo por disposición legal, cualquier entidad que trate datos personales se convertirá en responsable de aquello que suceda con los datos personales objeto de su tratamiento y; por lo tanto, debe dar una explicación adecuada y razonable en caso de que se produzca un incidente de seguridad respecto de estos. Y como se ha dicho anteriormente, ser capaz de demostrar dicho cumplimiento, merced al principio de responsabilidad proactiva previsto en el artículo 5.2 RGPD. Ahora bien**,** en cuanto a las herramientas que trago consigo el artículo 32 RGPD, habrá de ser complementado con otros en materia de seguridad , como ha de hacerse un análisis de riesgos, la implementación de la protección de datos desde el diseño y por defecto (articulo 25 RGPD) la necesidad de realizar una evaluación de impacto relativa a la protección de datos personales (artículo 35 RGPD) (CARRUZO 2022).

[16] Véase Art 32: Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, (…)

[17] Véase Art 5.1 f: Los datos personales serán tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, (…)

2.3.1. Análisis de riesgos

Dentro de este marco, ante la falta de una definición legal clara en el nuevo RGPD , la Guia de Gestión de riesgos, elaborado por el Instituto Nacional de Ciberseguridad (INCIBE) [18] conceptualiza la definición de análisis de riesgo, exterioriza que se trata de determinar el nivel de riesgo que la empresa está enfrentando, lo que tradicionalmente se logra mediante la realización de un inventario de activos, la identificación de amenazas, la evaluación de las probabilidades de que ocurran y la valoración de los posibles impactos. (INCIBE. 2015.Gestión de riesgos). Es importante contar con una metodología apropiada que establezca los niveles de riesgo aceptables para cada situación. El artículo 24 y 32 del RGPD, se considera como el punto de partida para cualquier actividad que involucre el tratamiento de datos personales, en lo referente a las obligaciones del responsable y a la seguridad de los datos. En efecto, la AEPD ha publicado una guía práctica como «gestión del riesgo y evaluación de impacto» (AEPD.2021. Guia práctica de análisis de riesgos y evaluación de impacto) que detalla el método a seguir, proporcionando modelos y formularios en abundancia (COTE 2020).

La primera fase del proceso de gestión de riesgos consiste en identificar los mismos. El riesgo no es sino una consecuencia de la exposición frente a amenazas. Una amenaza alude a todo factor de riesgo con potencial para provocar un daño o perjuicio a los titulares de los datos personales objeto de tratamiento; es decir, a los interesados. Las amenazas pueden clasificarse en tres tipos:

1.- Acceso ilegitimo de datos: haciendo referencia al daño que provocaría que los datos personales fueran conocidos por individuos no autorizados, afecta la dimensión de la confidencialidad.

2.- Modificación no autorizada de los datos, que causaría que el dato personal estuviera dañado, afectando la dimensión de la integridad.

3.- Eliminacion de los datos, afectando a la dimensión de la disponibilidad.

[18] Instituto Nacional de Ciberseguridad de España (INCIBE),

El nivel de riesgo se determina en base a la probabilidad y el impacto que podría causar en caso de suceder. La segunda etapa del proceso de gestión de riesgos consiste en evaluarlos, considerando todos los escenarios posibles en los que el riesgo podría materializarse. Se valora el impacto potencial de la exposición a la amenaza, así como la probabilidad de que esa amenaza se haga efectiva. El impacto se mide según los perjuicios que podrían derivarse si la amenaza se materializa. La tercera etapa del proceso es tratar los riesgos, lo cual implica aplicar medidas de control para reducir su probabilidad o impacto y disminuir el nivel de exposición. El riesgo inherente puede ser mitigado para reducirlo, de manera que su nivel llegue a ser residual a un nivel considerado como adecuado y razonable (AEPD.2021. Guia análisis de riesgos y Evaluación de impacto).

Partiendo de los supuestos anteriores, en toda metodología de análisis de riesgos, existe una fase en la que es necesario realizar una valoración de los activos y; para ello, se estiman las consecuencias hipotéticas que se tendrían que asumir en el supuesto de que se produjera un incidente que afectase a estas dimensiones. Para ello, se emplean diferentes critrios de valoraciones o escalas, que atienden a las diferentes perspectivas o contextos en los que el incidente de seguridad generaría daños. Las mas habituales son:

1.- Escala operativa: Mide las consecuencias que puede tener para la generación de valor o la prestación de servicios de negocio de la organización.

2.- Escala Legal: Mide las consecuencias derivadas del posible incumplimiento de alguna regulación o legislación que vele por garantizar la seguridad de la información como por ejemplo: la legislación en materia de protección de datos personales emanada a día de hoy, del RGPD, a nivel comunitario y de la nueva LOPDGDD[19] y a nivel interno español.

3.- Escala reputacional: Mide las consecuencias traducidas en daño de imagen que podría padecer la organización en el supuesto de sufrir una contingencia o incidente que afectará a la seguridad de la información.

Es por eso que la evaluación de riesgos debe resultar de una reflexión sobre las implicaciones que los tratamientos de datos personales que se pretenden llevar a cabo puedan tener en los

[19] Ley Orgánica 3/2028, 5 de diciembre, de Proteccción de Datos Personalesy garantía de los derechos digitales.

titulares de dichos datos. En definitiva, se trata de determinar hasta qué punto una actividad de tratamiento, dependiendo de sus características, del tipo de datos personales que se manejen o del tipo de operaciones, podría generar algún daño a los interesados. Por lo tanto, este enfoque requiere una estimación del daño y del tipo de daño que se podría ocasionar a los titulares de los datos. Debido a que el Responsable del Tratamiento es el que tiene la carga de la prueba, se recomienda documentar la gestión del riesgo (FERNANDEZ, 2011).

El proceso de identificación, análisis y gestión del riesgo pasa por una serie de actividades que ilustra la propia norma ISO 27005:2008. La idea de este apartado es explicar la relevancia del análisis de riesgos como medida de cumplimiento de la accountability.

2.3.2. Evaluación de impacto

En el contexto del RGPD, se introduce el término Evaluación de Impacto (artículo 35) relativa a la Protección de Datos, en adelante (EIPD). La AEPD, citando al Comité Europeo de Protección de Datos (CEPD)[20], explica que la EIPD es un proceso diseñado para describir el tratamiento, evaluar su necesidad y proporcionalidad, y ayudar en la gestión de los riesgos para los derechos y libertades de las personas físicas derivados del tratamiento de datos personales, mediante la evaluación de los mismos y la determinación de medidas para abordarlos.[21]

La (EIPD) es un análisis que se realiza durante todo el proceso de tratamiento de datos personales y que debe ser actualizado de manera regular, especialmente en caso de cambios en el riesgo que implican las operaciones de tratamiento. La EIPD ayuda al Responsable del Tratamiento o al Encargado del Tratamiento en la identificación, análisis y minimización de los riesgos que pueden presentarse durante el tratamiento de datos personales en una organización. Asimismo, permite implementar soluciones innovadoras y evaluar la viabilidad del plan desde una etapa temprana (MORALES 2022).

No se requiere realizar una (EIPD) para cada actividad de tratamiento, sino que es necesario evaluar si es necesario llevar a cabo dicha evaluación. Es esencial realizar un análisis previo

[20] Comité Europeo de Protección de Datos: Asegura que la legislación de la UE, especialmente el Reglamento General de Protección de Datos (RGPD) y la Directiva sobre protección de datos en el ámbito penal, se aplique de manera uniforme en todos los países regulados por ella, y fomenta la colaboración entre las autoridades nacionales de protección de datos.
[21] Ibídem, pag. 25

para determinar el nivel de riesgo asociado al tratamiento y tomar una decisión apropiada en consecuencia. Dependiendo de los resultados del análisis, podemos concluir si es necesario llevar a cabo una EIPD y documentar todo el proceso, o si no es necesario realizarla debido a que las actividades de tratamiento no están expuestas a riesgos relevantes. En este último caso, es importante documentar las razones que llevaron a tal conclusión y demostrar que se ha llevado a cabo un análisis proactivo, en línea con el principio de responsabilidad proactiva. (CORTIZAS DE CASTRO 2019).

Ahora bien cabe preguntarse, en que casos específicos se require realizar una (EIPD). En efecto, se puede seguir una breve metodología de análisis constituida en dos fases, la primera en análisis de listas de tratamiento previstos en la regulación (apartados 3,4,5) del artículo 35 RGPD[22]. La normativa de protección e datos incluye ciertos casos en los que es obligatorio realizar una evaluación de impacto. En efecto, el apartado tecero del artículo 35 del RGPD, recoge tres casos en los que es obligatorio realizar una (EIPD) «Evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado como la elaboración de perfiles y sobre cuya base se toman decisiones que produzcan efectos jurídicos para las personas físicas o que les afecta de modo similar», «tratamiento a gran escala de las categorías especiales de datos personales, o de datos sobre concenas e infracciones penales o medidas de seguridad conexas», «observación sistemática a gran escala de una zona de acceso público» . La segunda fase contenida en el apartado 1 del artículo 35 RGPD , que es el «Análisis de la naturaleza, alcance, contexto y fines del tratamiento(…)». Para ello, conceptualizaremos el significado de cada una. Sobre la naturaleza del tratamiento, es importante evaluar las características fundamentales del tratamiento y determinar si estas pueden conllevar un alto riesgo. Por ejemplo, es necesario analizar si se manejan categorías especiales de datos, si se emplean grandes cantidades de información, si se realiza un seguimiento detallado de los interesados, si se fusionan diversas conjuntos de datos o si los datos pertenecen a personas en situación de especial vulnerabilidad (CARRUZO 2022).

[22] Véase artículo 35 RGPD

En esta misma linea, sobre el alcance del tratamiento, es importante evaluar los efectos o resultados del tratamiento y determinar en qué medida pueden llegar a producir un riesgo significativo. Por ejemplo, se debe considerar si se va a tomar una decisión que tenga efectos legales, si se va a aplicar una valoración de riesgo crediticio, o si se evalúa la exclusión de beneficios sociales o fiscales. Sobre el contexto del tratamiento, es necesario considerar el conjunto de circunstancias en las que se llevarán a cabo las actividades de tratamiento, con el objetivo de determinar si podrían conllevar un riesgo significativo. Algunas circunstancias a considerar son el uso de nuevas tecnologías, las prácticas invasivas para la privacidad, la existencia de múltiples responsables de tratamiento, cadenas complejas de encargados de tratamiento, transferencias internacionales de datos personales, y la cesión de datos, entre otras. Y por ultimo las finalidades del tratamiento, es importante identificar cada uno de los propósitos del tratamiento y examinar si implican un riesgo significativo, por ejemplo, si el propósito implica la toma de decisiones, la elaboración de perfiles, la prestación de servicios relacionados con la salud, el seguimiento o la observación de personas (monitorización), entre otros (CARRUZO 2022).

Según las regulaciones actuales sobre protección de datos, se debe elaborar una (EIPD), cuando un tratamiento pueda implicar un alto riesgo para los derechos y libertades de los interesados, incluyendo aquellos reconocidos como fundamentales por la legislación, como el derecho a la protección de los datos personales, según lo establecido en la Carta de los Derechos Fundamentales de la Unión Europea. Esto se aplica especialmente cuando se utilizan nuevas tecnologías, teniendo en cuenta factores como la naturaleza, el alcance, el contexto o los objetivos del tratamiento (tal como se describe en el artículo 35.1 del RGPD y en la consideración 76 del mismo reglamento) explicado anteriomente (FERNANDEZ , LLORENS 2011).

Además, para identificar qué tratamientos pueden presentar un riesgo significativo, el GT29 incluyó en el Documento (WP2448) Directrices sobre las Evaluaciones de Impacto en la Protección de Datos, criterios que permiten identificar actividades de tratamiento con un riesgo inherente y alto, lo que requiere llevar a cabo una Evaluación de Impacto en la Protección de Datos (EIPD). Según el GT29, si un tratamiento cumple con más criterios, tendrá más probabilidad de representar un riesgo elevado para los derechos y las libertades de los

titulares de los datos. Sin embargo, en algunos casos el responsable del tratamiento puede considerar que, a pesar de cumplir varios criterios, no existe una probabilidad alto riesgo debido a la naturaleza del tratamiento. En estos casos, será necesario documentar y argumentar claramente las razones por las que no se lleva a cabo la evaluación de impacto.

Aunque la lista de criterios es abierta, esto no excluye la necesidad de llevar a cabo una Evaluación de Impacto en otros casos que también puedan presentar riesgos elevados. Será importante elaborar un informe que detalle los criterios utilizados y los argumentos que sustentan la conclusión sobre la necesidad o no, de realizar la EIPD.

2.4. Protección de datos desde el diseño y por defecto

En esta sección, abordaremos el concepto de protección de datos desde el diseño y por defecto, que es un elemento clave para determinar los medios del tratamiento establecido por el RGPD. Nos enfocaremos en aspectos importantes, como su naturaleza y definición, su relación con el análisis de riesgos, la regulación correspondiente, los sujetos obligados, las estrategias para su aplicación.

En primer orden, el artículo 25 del RGPD, define la protección de datos desde el diseño y por defecto; a su vez, el considerando 78 y 108 Ibidem, lo señalan como principios, lo mismo ocurre con la accountability, en la interpretación y la practica del RGPD. Siendo así, debería incluise en el apartado del artículo 5 dedicado a principios. Continuando con este análisis, desde el inicio o implementación de los tratamientos, existe una exposición a los riesgos que pueden afectar al ámbito de la protección de datos. Estos riesgos pueden evolucionar a lo largo del tiempo y dependerán de los cambios en el contexto y los factores involucrados en los tratamientos.

Estamos hablando del principio de seguridad que es un concepto esencial establecido en la mayoría de las normas de protección de datos personales. Su aplicación es extendida en todo el mundo y suele cumplirse independientemente de que exista una conciencia explícita en cuanto a la protección de datos. La seguridad informática es una necesidad básica para cualquier organización, no sólo para la protección de datos, sino también porque existe la posibilidad de ataques maliciosos, la necesidad de proteger secretos empresariales, secretos

de Estado, patentes, marcas, entre otros. El principio de seguridad es relevante en cualquier organización, ya sea pública o privada (SANTAMARIA 2020).

Este principio implica que el responsable del tratamiento debe implementar políticas, medidas y protocolos, tanto técnicos como organizativos y legales, para garantizar la seguridad de los datos personales. Este es el punto clave del principio de protección desde el diseño y por defecto. Significa que tanto las organizaciones públicas como privadas, y especialmente algunas organizaciones sectoriales, deben incentivar a la industria tecnológica para que, cuando diseñen y desarrollen productos, servicios o aplicaciones que involucren el tratamiento de datos personales lo hagan pensando siempre en los responsables y encargados del tratamiento como figuras clave de cualquier normativa de protección de datos personales. De esta forma, podrán cumplir de manera adecuada con la normativa en materia de protección de datos personales (SANTAMARIA 2020).

2.4.1. Privacidad desde el diseño

El apartado primero del artículo 25 del RGPD regula la protección de datos desde el diseño-PbD- y en el considerando 78 íbidem. Aplicará en el momento de determinar los medios del tratamiento, como en el momento propio, medidas técnicas y organizativas e integrar las garantías adecuadas[23]. Por otra parte, el segundo apartado establece la regulación sobre la protección de datos por defecto, que obliga al responsable del tratamiento a implementar medidas técnicas y organizativas para asegurar que sólo se traten los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento, por defecto.[24]

Los dos conceptos tienen un propósito claro: asegurar los derechos y libertades de los titulares de datos personales desde la misma definición de una actividad de tratamiento específica. Por lo tanto, el responsable del tratamiento que realice o tenga planeado llevar a cabo actividades de tratamiento con datos personales debe establecer procedimientos de control que permitan cumplir con los principios de protección desde el diseño y por defecto. Ahora bien, la AEPD, ha determinado en la guía de Privacidad desde el diseño (Agencia Española de Protección de Datos 2019) en torno al trabajo realizado bajo la terminologia de privacidad

[23] Véase art. 25.1 y considerando 78 del RGPD
[24] Véase art. 25.2 y considerando 108 del RGPD

desde el diseño (Privacy by Design,o PbD), realizado por la comisionada de Protección de Datos de Ontario Canada[25] Ann Cavoukian, que define siete principios a trabajar activamente:

1. «Proactivo, no reactivo; Preventivo, no correctivo» Consiste en anticiparse a los eventos que afecten a la privacidad antes de que sucedan. La PbD huye de la "política de subsanar" ¿Cómo lo hago? Concibiendo y diseñando desde cero el sistema o tecnología, identificando los posibles riesgos y amenazas a los derechos y libertades de los interesados antes de que puedan concretarse en daños.
2. « La privacidad como configuración predeterminada». Proporciona al usuario el máximo nivel de privacidad, se fundamenta en la minimización de datos ¿En que se concreta? En definir plazos de conservación y establecer mecanismos operativos para ello. Crear barreras tegnológicas que impidan la vinculación no autorizada de fuentes de datos independientes.
3. « Privacidad incorporada en la fase de diseño». Garantizar la privacidad desde las primeras etapas del diseño, ejecutar un análisis de riesgos y evaluaciones de impacto, y documentar las decisiones que se adopten en el seno de la organización ¿En que se concreta? En considerar como un requisito necesario en el ciclo de vida de sistemas y servicios.
4. « Funcionalidad total: pensamiento todos «ganan». Tradicionalmente se ha creído que tener privacidad implica perder otras funciones. Sin embargo, esta idea es falsa y el objetivo debe ser buscar un equilibrio óptimo en una búsqueda "ganar-ganar" ¿En que se concreta? En establecer canales de comunicación para colaborar y consultar a las partes interesadas con el objeto de comprender múltiples intereses.
5. « Aseguramiento de la privacidad en todo el ciclo de vida» La privacidad nace en el diseño, antes de que el sistema esté en funcionamiento, y debe garantizarse durante todo el ciclo de vida. La seguridad de la información impone confidencialidad, integridad y disponibilidad y resiliencia de los sistemas ¿En que se concreta? En la seudonimización temprana, el cifrado por defecto de modo que el estado "natural" de

[25] En la década de los 90; presentado en la 31ª Conferencia Internacional de Comisionados de Protección de Datos y Privacidad del año 2009 bajo el título "Privacy by Design: The Definitive Workshop

los datos en caso de pérdida o robo sea "ilegible" y la destrucción segura y garantizada de la información al final del ciclo de vida.

6. « Visibilidad y transparencia» Una de las claves para garantizar la privacidad es poder demostarla, verificando que el tratamiento es acorde a la información que se esta recogiendo, utilizando, consultando. ¿En que se concreta? En políticas de privacidad y cláusulas de información concisas, claras y accesibles. Establecer mecanismos de comunicación sencillos dirigidos a los titulares de los datos.
7. Respeto por la privacidad de los usuario: «Mantener un enfoque centrado en el usuario» El objetivo principal debe ser asegurar los derechos y libertades de los usuarios cuyos datos están siendo sometidos a tratamiento, por lo que cualquier medida que se adopte tiene que estar enfocada en preservar su privacidad.

Esto se refiere a la implementación de configuraciones de privacidad por defecto robustas y a informar a los usuarios sobre las posibles implicaciones en su privacidad en caso de que modifiquen dichas configuraciones. También se deben establecer mecanismos que permitan a los interesados ejercer sus derechos en protección de datos.

En relación a estas consideraciones, surge la pregunta acerca de quién debe aplicar la protección de datos desde el diseño. Aunque el responsable del tratamiento de los datos es quien tiene la obligación de cumplir con esta normativa, la protección de datos desde el diseño se extiende; además, a otros participantes que intervienen en el tratamiento de datos personales como proveedores, prestadores de servicios, desarrolladores, fabricantes de dispositivos, entre otros. Por lo tanto, las estrategias de privacidad pueden variar en función de cada caso (CARRUZO 2022).

En este caso, se condisera imperante analizar las estrategias de diseño de la privacidad que detallare a continuación como su significado, su táctica y los patrones de diseño:

ESTRATÉGIA	TÁCTICA	PATRONES DE DISEÑO
Minimizar: Tratar la mínima cantidad de datos.	• Eliminar parcialmente los datos personales tan pronto dejen de ser necesarios.	• Anonimización y pseudonimización.

Ocultar: Limitar la exposición de datos.	• **Restringir:** Limitar el acceso a datos personales, tanto el detalle y tipo de datos accedidos. • **Ofuscar:** Hacer que los datos personales no puedan visualizarse para no autorizados, mediante el cifrado y hashing. • **Disociar:** Eliminar la vinculación entre conjuntos de datos que se han de mantener independientes. • **Agregar:** Agrupar la información relativa a varios sujetos utiizando técnicas de supresión para evitar correlaciones	• El Cifrado
Separar: Evitar que diferentes datos personales pertenecientes a un mismo individuo y utilizados en tratamientos independientes, se	• **Aislar:** Almacenar los diferentes datos personales en diferentes bases de datos o aplicaciones que sean independientes.	• Listas negras • Anónimas, • cifrado.

pueda llegar a realizar un perfilado.		
Abstraer: Limitar al máximo los detalles de datos que son tratados.	• Agregación en el tiempo.	• Privacidad referencial
Informar: Los interesados estén informados del procesamiento de sus datos en tiempo y forma. Debe ser accesible.	• Debe ser fácilmente accesible • Comunicar el tratamiento a los interesados.	• Usar modelo de información por capas
Demostrar: A los interesados y a las autoridades de supervisión el cumplimiento de la política de protección de datos		

(AEPD. 2019. Guia de privacidad desde el diseño).

En conclusión, el proyecto del RGPD promueve la protección de datos desde el diseño y por defecto (Privacy by Design y Privacy by Default), obligando a las entidades que manejen datos -teniendo en cuenta las técnicas existentes y los costos de su implementación- a implementar medidas y procedimientos técnicos y organizativos apropiados para que el tratamiento de datos cumpla la normativa de protección de datos. En particular, estas medidas deben garantizar la protección de los derechos individuales, limitar el tratamiento de los datos personales a lo estrictamente necesario para cada fin, preservar los datos por el tiempo y

cantidad mínimos necesarios (el principio de minimización de datos) y evitar que sean accesibles al público por defecto. Además, la Comisión puede emitir actos delegados sobre nuevos criterios y requisitos para garantizar la protección de datos desde el diseño, y actos de ejecución que especifiquen las normas técnicas (RALLO 2012).

2.4.2. Privacidad por defecto

El concepto de Protección de datos por Defecto, también conocido como (PDpD), se encuentra definido en el artículo 25.2 y en la consideración 78 del RGPD. Al igual que con la Privacidad desde el Diseño (PbD), nuestro enfoque se basará en la guía proporcionada por la AEPD (Agencia Española de Protección de Datos) para la aplicación de la privacidad por Defecto.

El artículo 25 del (RGPD) indica que los principios, derechos y obligaciones relacionados con la protección de datos contenidos en dicho Reglamento deben considerarse desde el diseño y por defecto. De esta manera, la implementación efectiva de la protección de datos por defecto se convierte en una de las medidas de responsabilidad proactiva que ayuda a demostrar el cumplimiento de las obligaciones establecidas en la normativa.

En consecuencia, el RGPD exige que el responsable establezca una configuración predeterminada para los procesos de tratamiento de datos que cumpla con los principios de protección de datos (art.5) , favoreciendo un procesamiento que sea lo menos intrusivo posible: 1.- Minima cantidad de datos (Principio de minimización)[26], 2.- Mínima extensión del tratamiento (principio de limitación de la finalidad) [27], 3.- Mínimo plazo de conservación (Principio de limitación del plazo de conservación)[28] 4.- Mínima accesibilidad a los datos personales (Principio de integridad y confidencialidad)[29].

En este contexto, la selección de medidas y garantías para la - PDpD- tinene influencia sobre los requisitos que se imponen en los ámbitos de seguridad (confidencialidad, disponibilidad, integridad y autenticidad) desde la perspectiva de la "seguridad por defecto". En síntesis, el (art 25.2) del RGPD determina «Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número

[26] Véase artículo (5.1. c)
[27] Véase artículo (5.1.b)
[28] Véase artículo (5.1.e)
[29] Véase artículo (5.1.f)

indeterminado de personas físicas» En consecuencia, se opta por la conocida "Política de míminos privilegios".

Ahora bien, presentamos una distinción en cuanto al análisis de riesgos. Este análisis es un requisito fundamental antes de implementar cualquier medida en cumplimiento del RGPD, incluidas aquellas relacionadas con los principios del artículo 25 del RGPD. No obstante de aquello, en lo que se refiere a la privacidad por defecto, las medidas para su implementación no dependerán del análisis de riesgos, ya que se adoptarán "por defecto" como una medida preventiva, independientemente del resultado de dicho análisis. (AEPD.Guía de Protección de Datos por Defecto) En cuanto al aspecto temporal, la (PbD) debe ser implementada antes del proceso de tratamiento, de manera que las medidas por defecto se integren como parte del sistema de protección.

En este orden de ideas, la opinión fijada por el Comité Europeo de Protección de Datos con relación a la implementación de medidas de PDpD se centra en tres estrategias:

1.- Optimizar: La optimización del procesamiento busca examinarlo en términos de protección de datos, lo que implica implementar medidas que consideren la cantidad de datos recopilados, la amplitud del procesamiento su retención y accesibilidad.

2.- Configurar: Esta táctica tiene que posibilitar la configuración del manejo de datos personales a través de ajustes disponibles en las aplicaciones, dispositivos o sistemas que lo ejecutan. Una parte de esa capacidad de configuración debe estar en manos del usuario.

3.- Restringir: La limitación asegura que de forma predeterminada, el procesamiento sea lo más respetuoso posible con la privacidad, por lo que las opciones de configuración deben estar ajustadas de manera predeterminada a valores que restrinjan la cantidad de datos recopilados, el alcance del tratamiento, su retención y accesibilidad.

2.5. El delegado de Protección de Datos

En esta sección, nos enfocaremos en examinar el rol del Delegado de Protección de Datos, (en adelante DPO) una figura esencial en el marco de protección del RGPD basado en el principio de accountability. Discutiremos de manera concisa sus cualidades profesionales, fomaliades de designación y sus funciones , así como los aspectos vinculados a su nombramiento.

En primer lugar, es importante destacar que en la Directiva 95/46/CE permitía a los Estados miembros de la Unión Europea (en adelante UE) decidir si legislaban o no acerca del Delegado de Protección de datos, ya que no se contemplaba la figura como tal. Como resultado de la Directiva 95/46/CE, los Estados miembros de la UE han abordado de manera individual la cuestión del DPO en su legislación, lo que ha creado un marco legal desigual, con algunos Estados que han regulado esta figura y otros que no han mencionado al DPO en sus normativas. Esta disparidad busca ser corregida con el nuevo RGPD (Monzón 2017).

Por lo tanto, en este apartado se examinarán de manera resumida las disposiciones normativas que introduce el RGPD acerca del DPO, y las novedades que plantea al respecto el proyecto de ley que busca adaptar la Ley Orgánica de Protección de Datos Personales española a la nueva normativa europea.

Al respecto, el RGPD que es directamente aplicable sin necesidad de ser transpuesto, se crea en el ámbito de la UE con el propósito de proporcionar criterios uniformes y coherentes que garanticen seguridad jurídica, cuyas normativas son de aplicación directa en todos los estados miembros de la UE y tienen plenos efectos juridicos. En este sentido, se incluye en su sección 4 las disposiciones referentes al DPO. En los artículos 37, 38 y 39 del RGPD se detallan la designación, la posición y las funciones del DPO, y en los artículos 34 al 37 de LOPDGDD respectivamente.

Es oportuno precisar que el RGPD define el significado y la extensión de los conceptos involucrados en la normativa; no obstante, no proporciona una definición del DPO. Para este efecto, la definición presentada por el documento sobre la evaluación de impacto de la Comisión Europea en relación con la propuesta del reglamento es más detallada en comparación. Aunque no menciona explícitamente el tipo de capacitación requerida para la persona que ocupe dicho cargo, la traducción al español de la definición en inglés es más precisa, se traduce como « aquella persona, responsable en el seno de un responsable o de

un encargado del tratamiento, de realizar la supervisión y monitorización, de forma independiente, de la aplicación interna y de garantizar el respeto a las normas en materia de protección de datos personales, pudiendo ser desempeñado tanto por un empleado interno como por un consultor externo »(Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the protection of individuals 2012).

Ahora bien, una vez definido el concepto de DPO, antes de la entrada en vigor del RGPD, el GT29 sostenía que el DPO es fundamental para la rendición de cuentas, y que designar a un DPO puede facilitar el cumplimiento normativo y, asimismo, ser una ventaja competitiva para las empresas. Además de favorecer el cumplimiento a través de la implementación de mecanismos de rendición de cuentas (como realizar evaluaciones de impacto y auditorías de protección de datos), los DPO actúan como intermediarios entre las partes interesadas relevantes (por ejemplo, autoridades de control, partes interesadas y unidades comerciales dentro de una organización) (GT29.WP243.p.4).

Atendiendo a estas consideraciones, el DPO puede ser interno o externo a la organización, es decir, puede ser un empleado contratado por el responsable del tratamiento (RT) o por el encargado del tratamiento (ET); a se vez, puede ser un prestador externo a través de un contrato de servicios.[30] Es importante destacar que, independientemente de su situación, el DPO no recibirá instrucciones ni órdenes para ejercer su cargo, ya que debe actuar como una figura independiente. [31]Su responsabilidad consistirá en garantizar el cumplimiento en el tratamiento de datos dentro de la organización y asesorar tanto al RT, ET, como al personal de la empresa en temas relacionados con la protección de datos, además de sensibilizar y supervisar el cumplimiento de la normativa. De la mis forma, el DPO será un intermediario entre los interesados con la autoridad de control.

Además, la regulación de esta figura también incluye un enfoque en la gestión de riesgos. El DPO tiene la responsabilidad de ser diligente en el ejercicio de sus funciones, lo que implica

[30] Véase:art 37.6 (RGPD)
[31] Véase:art 38.3 (RGPD)

prestar la debida atención a los riesgos asociados con los procesos de tratamiento, considerando la naturaleza, alcance, contexto y propósitos del tratamiento[32].

Cualidades profesionales y competencias DPO

En relación a los requisitos, habilidades, perfil profesional, experiencia y formación que debe tener un (DPO), tanto la (LOPDGDD) como el (RGPD) establecen diversas especificaciones, detalladas principalmente en el artículo 37.5 del RGPD y en los artículos 34 y 35 de la LOPDGDD.

El DPO será seleccionado y designado en función de sus capacidades profesionales, especialmente su formación y experiencia especializada en derecho y protección de datos. Se hace énfasis en la experiencia práctica en el campo y la habilidad para desempeñar las funciones requeridas. Puede ser una persona física o jurídica, y su carga de trabajo puede ser a tiempo completo o parcial, dependiendo de la complejidad, el volumen de datos tratados, la categoría de los datos manejados y los riesgos para los derechos y libertades de los interesados. Ahora bien, continuando con la normativa citada, podemos identificar los siguientes criterios necesarios para ser designado como DPO:

1.- Especialización

El DPO debe poseer una amplia comprensión de la legislación nacional, europea e internacional en el ámbito de protección de datos. Es fundamental poseer un entendimiento de las operaciones específicas de tratamiento que se llevan a cabo dentro de la organización, así como mantenerse actualizado en la tecnología de seguridad de datos. El DPO, deberá estar en formación permanente, para poder conocer las aplicaciones informáticas y sobre el procesamiento de la información.El grado de especialización requerido dependerá de la organización en cuestión, del volumen y complejidad de los datos procesados y si existe transferencia internacional de datos (considerando 97 del RGPD). La LOPDGDD añade que los requisitos necesarios para ser nombrado DPO podrán ser "demostrados" a través de diversos medios, incluyendo mecanismos de certificación voluntarios que consideren especialmente la

[32] Véase:art 39.2 (RGPD)

obtención de un título universitario que avale conocimientos especializados en derecho y experiencia práctica en materia de protección de datos.[33]

En la actualidad, AEPD junto con la Entidad Nacional de Acreditación (ENAC) y la participación de un Comité Técnico de Expertos (representantes de diversos sectores, asociaciones profesionales, empresas, universidades y Administraciones Públicas), ha desarrollado el Esquema de Certificación de Delegados de Protección de Datos basado en la norma ISO 17024 (requisitos generales para las entidades que realizan la certificación de personas). Este sistema de certificación proporciona confianza y asegura la calidad a los profesionales de privacidad, a las empresas y entidades que integran esta figura en sus organizaciones, a través de un proceso que garantiza que los Delegados cuentan con la formación profesional y los conocimientos necesarios. Es importante mencionar que esta certificación no es obligatoria para ejercer como Delegado (SIERRA 2018).

2.- Capacidad para su desempeño en la materia

En la industria, se espera que el (DPO) cuente con un perfil académico avanzado, que incluya al menos un grado universitario, seguido de un doctorado o máster. Además, se requieren certificaciones reconocidas, un alto nivel de dominio del inglés, experiencia previa en el ámbito de la protección de datos, así como conocimientos especializados en derecho y tecnologías de la información (hard skills)[34].

Adicionalmente, se valoran una serie de cualidades personales, como proactividad, creatividad, asertividad, visión global, capacidad de impactar e influenciar, habilidades de análisis y planificación, formación continua, trabajo en equipo, accesibilidad, transversalidad, empatía y habilidades de comunicación (soft skills)[35] (SIERRA 2018).

[33] Véase artículo 35 LOPDGDD

[34] Incibe: hard skills, también conocidas como habilidades duras o habilidades técnicas, se refieren a las competencias técnicas específicas que una persona posee para llevar a cabo una tarea dentro de su entorno laboral. Generalmente, estas habilidades se adquieren durante la etapa formativa, como en un grado superior o universitario, y se perfeccionan a lo largo de la experiencia profesional. Véase: https://www.incibe.es/ed2026/talento-hacker/blog/habilidades-en-ciberseguridad-skills-y-soft-skills

[35] Incibe: Conocidas como habilidades blandas, estas se refieren a las competencias no técnicas que suelen tener un aspecto más personal. A diferencia de las hard skills, las soft skills se pueden aprender y mejorar mediante la experiencia y la práctica ejm liderazgo.

Es notable que actualmente son limitadas las universidades y escuelas de negocios que ofrecen programas formativos en Derecho y Tecnología de datos que proporcionen las competencias personales y profesionales necesarias para el desempeño de los roles requeridos en la Industria. Respecto al DPO, las Directrices sobre Delegados de Protección de Datos (DPD) el GT29 indican que el nivel de conocimiento debe ser apropiado para la sensibilidad, complejidad y volumen de datos que maneja una organización. Por lo tanto, la elección del DPO debe hacerse cuidadosamente, considerando detenidamente los aspectos relacionados con la protección de datos en la organización. En cuanto a las cualidades profesionales, es crucial que el DPO tenga conocimiento de la legislación y prácticas nacionales y europeas en materia de protección de datos, una comprensión profunda del RGPD, así como del sector empresarial y la estructura de la organización del responsable del tratamiento. Además, se requiere un buen entendimiento de las operaciones de tratamiento y protección de datos del responsable del tratamiento(SIERRA 2018).

La doctrina ha señalado que en el caso de un (DPO) que forme parte de organizaciones del ámbito privado, además de comprender el sector empresarial, el DPO debe poseer un conocimiento detallado del modelo de negocio de la organización, especialmente cuando este se fundamenta en el tratamiento de datos personales. Esto permitiría fomentar la innovación y la competitividad de la organización al mismo tiempo que se garantiza el derecho fundamental a la protección de datos personales.

2.5.1. Posición del Delegado de Protección de Datos

Según el artículo 38.1 del RGPD, se establece que tanto el responsable del tratamiento como el encargado del mismo deben asegurar la participación oportuna y adecuada del (DPO) en todos los asuntos relacionados con la protección de datos personales.

Como se ha mencionado, el DPO desempeña un papel clave al coordinar diversas áreas de la empresa como Recursos Humanos, Seguridad Corporativa, Legal, Marketing, Comercio Electrónico, Financiero o Auditoría. La importancia de la posición del DPO ha sido abordada en una de las Directrices del Grupo de Trabajo sobre Protección de Datos del Artículo 29 (GT29), resaltando la necesidad de que el DPO, o su equipo, participen desde las etapas iniciales en todos los asuntos relacionados con la protección de datos. Asegurando el cumplimiento efectivo del RGPD y el principio de proactividad, que implica planificar, ejecutar, verificar y actuar, conocido como el ciclo Deming (PDCA), una metodología adoptada por los

estándares internacionales[36] de las normas ISO relacionadas con la planificación, acción y supervisión en el cumplimiento normativo. El GT29 introduce una directriz fundamental que establece que, para facilitar el cumplimiento «compliance» con el Reglamento y asegurar la implementación de la privacidad desde el diseño, las organizaciones deben incluir como parte de su gobernanza el proceso de informar y consultar al DPO.

El responsable del tratamiento o el encargado estarán obligados a involucrar al DPO de la siguiente manera: se solicita la participación regular del DPO en reuniones con los altos y medios directivos. Se sugiere su presencia cuando se tomen decisiones con implicaciones en la protección de datos. Toda la información relevante debe ser compartida con el DPO y se considera su opinión. En caso de desacuerdo, el grupo de trabajo recomienda como buena práctica documentar las razones por las cuales no se tomó en cuenta la opinión del DPO.

El DPO desempeña un papel crucial en la rendición de cuentas, ya que se anticipa que informe directamente la cúpula directiva de mayor nivel, ocupando una posición de importancia estratégica en el desarrollo de la organización o empresa. Para que el DPO alcance el éxito y desempeñe eficazmente sus responsabilidades, es esencial que la alta dirección de la empresa impulse y cultive una mentalidad y cultura de protección de datos (GT29.WP243.p 4).

Por otra parte, el DPO, en el ejercicio de sus responsabilidades, tendrá autorización para acceder a los datos personales y a los procesos de tratamiento, sin que el responsable o el encargado del tratamiento puedan oponerse a este acceso invocando deberes de confidencialidad o secreto.

En caso de que el DPO identifique una violación relevante en la protección de datos, debe informar de inmediato a los órganos de administración y dirección del responsable o del encargado del tratamiento[37] . Para concluir, es importante destacar una serie de garantías esenciales relacionadas con el ejercicio de sus funciones de manera independiente, así como la prohibición de despido o sanción por el cumplimiento de dichas funciones.

Con respecto al conflicto de intereses, ROMERO(2020)siguiendo a Sonia Marín determina que, para prevenir posibles conflictos de interés y, por ende, evitar motivos de sanción, las

[36] International Organization for Standartization
[37] Véase artículo 34 LOPDGDD

empresas deben externalizar el servicio o contar con el respaldo de otras empresas especializadas en el ámbito de la protección de datos.

En este contexto, es oportuno indicar que la Resolución de la Autoridad de Control Belga, el 28 de abril de 2020, impuso una multa de 50.000 euros a una empresa por no cumplir con la obligación de prevenir un conflicto de intereses según lo establecido en el artículo 38 del RGPD (PwC Tax&Legal Services 2020).

2.5.2. Formalidadades de la Designación

Sobre la designación del DPO, es siempre recomendable designar a un DPO, ya sea de manera obligatoria o voluntaria. En el caso de enfrentarse a una posible sanción, la AEPD podría considerar como atenuante el hecho de contar con un DPO de forma voluntaria y, como agravante, el no haberlo designado cuando era obligatorio. Además, esta figura está destinada a facilitar la comprensión de la extensa normativa en materia de protección de datos, siendo una medida que permite cumplir con las normas y demostrar el principio de responsabilidad (accountability).

2.5.3. Funciones

Las responsabilidades del DPO son diversas y están descritas en el artículo 39 del RGPD y en los artículos 36 y 37 de la LOPDGDD. Se detallará las siguientes:

1.- Funciones organizativas: El DPO debe establecer y mantener un registro de las actividades de procesamiento de datos personales, lo que garantiza el cumplimiento del principio de responsabilidad proactiva. Además, debe revisar las actividades de procesamiento registradas para asegurarse de su conformidad con el RGPD y participar en las Evaluaciones de Impacto de Protección de Datos (EIPD) si se llevan a cabo correctamente.

2.- Funciones de supervisión: La supervisión del cumplimiento del RGPD por parte de la organización es continua para el DPO. Debe gestionar las violaciones de seguridad de datos personales, informar a la Agencia Española de Protección de Datos (AEPD) y a los interesados en caso de una violación que ponga en riesgo sus derechos y libertades. También puede investigar iniciativas propias o a solicitud de la organización o de cualquier individuo en asuntos relacionados con sus responsabilidades, informando los resultados de dichas investigaciones.

3.- Funciones consultivas: El DPO proporciona asesoramiento sobre las obligaciones de protección de datos tanto al responsable del tratamiento (RT) como al encargado del tratamiento (ET) y al personal con acceso a datos. Ofrece recomendaciones sobre evaluaciones de impacto, mejoras y actualizaciones de políticas y prácticas de protección de datos de la organización. Puede recomendar la implementación de códigos de conducta y la obtención de certificaciones en protección de datos.

4.- Funciones informativas: Debe diseñar programas de formación y concienciación para el personal.

Como se puede inferir, en relación a las responsabilidades de las organizaciones y empresas en cuanto a la protección de los datos personales, el Tribunal Supremo de la Sala de lo Contencioso-Administrativo confirmó una multa de 40.001 euros a un responsable del tratamiento, (compañía Commcenter) dedicada a la compra y venta de productos de telefonía por la vulneración del principio de seguridad de los datos personales, ya que estaba obligada a adoptar de manera efectiva, las medidas técnicas y organizativas que impidan el acceso no autorizado por parte de terceros a los datos personales que constan en sus ficheros y la entidad incumplió esta obligación denominada de resultado, por los contratos de financiación de 14 particulares que contenían datos personales: nombres, domicilios, teléfonos, estado civil, familiares a cargo, ingresos, situación laboral, cargos, números de cuentas corrientes, importes financiados, mensualidades y la firma del contratante, se enviaron a un tercero ajeno a la relación contractual, por no implementar las medidas técnicas necesarias para asegurar la seguridad de los datos. Esta reciente sentencia ha establecido un precedente, indicando que la obligación del responsable del tratamiento es de medios, de conducta o diligencia debida, siendo suficiente adoptar medidas técnicas y organizativas y llevar a cabo una gestión diligente en su implementación con los medios apropiados y adecuados. Según la sentencia del Tribunal Supremo, la responsabilidad de las empresas para garantizar la seguridad de los ficheros que contienen datos personales de sus clientes es de medios y no de resultados. Esto significa que las empresas deben establecer medidas técnicamente apropiadas para proteger los datos, y utilizarlas de manera razonable, sin que se les pueda exigir la obtención de un resultado perfecto en materia de seguridad. La responsabilidad de las empresas se limita a implementar las medidas de seguridad adecuadas, sin que puedan ser sancionadas por

eventuales brechas de seguridad que ocurran, siempre que hayan actuado de forma diligente (Tribunal Supremo 2022).

3. Conclusiones

En este trabajo de fin de máster se ha realizado un análisis jurídico del principio de responsabilidad proactiva o accountability. El objetivo ha sido clarificar su comprensión, profundizando en su significado y envergadura, así como en las responsabilidades que implica.

Esto se ha hecho con la finalidad de abordar la cuestión presentada, que es la complejidad de asimilar este principio para disminuir la inseguridad jurídica.

La complejidad se origina porque nos enfrentamos a un principio jurídico que presenta retos interpretativos. Además, considerando que la accountability se extiende a lo largo de todo el Reglamento General de Protección de Datos (RGPD), su comprensión resulta aún más imprescindible.

Una vez completado este trabajo, hemos llegado a las siguientes conclusiones que detallo a continuación:

PRIMERA. - Respecto al análisis del concepto de responsabilidad proactiva en el marco de la nueva legislación de protección de datos, se ha evidenciado la necesidad de delimitar su alcance y su interpretación. Se destaca la importancia de examinar el cumplimiento de este principio para garantizar el respeto a los derechos individuales y facilitar el flujo adecuado de datos entre empresas. La clarificación de este concepto jurídico previamente indeterminado es crucial para una aplicación efectiva de las normativas de protección de datos.

SEGUNDA. - En torno con los objetivos específicos abordados, se ha determinado que el compromiso para las personas jurídicas implica demostrar una protección efectiva que verifique el cumplimiento de las obligaciones normativas. Se ha enfatizado en aspectos clave como la seguridad, la privacidad desde el diseño y por defecto, así como el papel esencial del DPO en este proceso.

TERCERA. - Por otro lado, la creación de un conjunto de directrices en analogía con el tratamiento masivo de datos personales ha sido fundamental para superar las medidas existentes en términos legales, organizativos y técnicos. Estas directrices adicionales establecen límites claros sobre las acciones que deben llevarse a cabo, contribuyendo al

cumplimiento adecuado del Reglamento General de Protección de Datos (RGPD) a través de la accountability

CUARTA. - Tras analizar la gestión del riesgo, el análisis del riesgo, la evaluación de impacto, la privacidad desde el diseño y por defecto, así como el papel del delegado de protección de datos en el marco de la protección de datos personales, se puede concluir lo siguiente:

-La gestión del riesgo en el tratamiento de datos personales es fundamental para identificar, evaluar y mitigar posibles riesgos que puedan afectar la privacidad de los individuos. Implementar medidas de gestión del riesgo permite a las organizaciones anticiparse a posibles incidentes y garantizar un tratamiento adecuado de la información personal.

-El análisis del riesgo es un requisito esencial para cumplir con el Reglamento General de Protección de Datos (RGPD) y otras normativas de privacidad. Evaluar los riesgos asociados al tratamiento de datos permite tomar decisiones informadas sobre las medidas de seguridad y protección que deben implementarse para garantizar la confidencialidad e integridad de la información.

-La evaluación de impacto en la protección de datos es una herramienta clave para identificar y mitigar los riesgos que el tratamiento de información personal puede generar en una organización. Realizar una evaluación de impacto de forma proactiva permite gestionar adecuadamente los riesgos y garantizar el cumplimiento de las normativas de privacidad.

-La privacidad desde el diseño y por defecto implica integrar medidas de protección de datos en todas las etapas del ciclo de vida de un sistema o servicio. Esta aproximación garantiza que la privacidad sea una consideración central desde el inicio del diseño, evitando así posibles vulnerabilidades y protegiendo la información personal de forma predeterminada.

El DPO desempeña un papel crucial en la garantía del cumplimiento de las normativas de protección de datos dentro de una organización. Su función de asesoramiento, supervisión y coordinación en materia de privacidad contribuye a asegurar que se adopten las medidas necesarias para proteger los datos personales y cumplir con las obligaciones legales en este ámbito.

En definitva, la gestión del riesgo, el análisis del riesgo, la evaluación de impacto, la privacidad desde el diseño y por defecto, y el papel del delegado de protección de datos son elementos fundamentales para garantizar la protección efectiva de los datos personales y el

cumplimiento del RGPD, son medidas de cumplimiento de la accountability en un entorno cada vez más digitalizado y globalizado. Su correcta implementación y coordinación son clave para promover una cultura de respeto hacia la privacidad y seguridad de la información personal en las organizaciones.

En resumen, el estudio ha permitido avanzar en la comprensión y aplicación de la responsabilidad proactiva en la protección de datos, destacando la importancia de adoptar medidas concretas para garantizar el cumplimiento normativo y promover una cultura de respeto hacia la privacidad y seguridad de la información personal. Estos hallazgos refuerzan la necesidad de una gestión responsable de los datos en un entorno digitalizado y globalizado, donde la protección de la privacidad se rige como un pilar fundamental para el desarrollo sostenible de las organizaciones.

Referencias bibliográficas

Bibliografía básica

Libros

CARRUZO, V. «Seguridad del Tratamiento: Aspectos Técnicos parte 1 (80-82): En *Colección Monografías Protección de Datos Personales*». BOSCH EDITOR. Barcelona. 2022

MURGA, F. JP. Et al. *Protección de datos, responsabilidad activa y técnicas de garantía.*1 ED. Madrid: REUS, 2018.

FERNANDEZ S. J., MARIA DE LOS ANGELES, y ESPEJO M. *Protección de datos, responsabilidad activa y técnicas de garantía.*1 ed.Madrid:REUS, 2018.

HUESCA, E. 2019. «*Diccionario de Protección de Datos Personales conceptos fundamentales*» [en línea]. Primera. Colombia : Isabel Davara F. de Marcos. Disponible en: DICCIONARIO PDP digital.pdf (inai.org.mx) [accedido 30 abril 2024].

Revistas

ZAMIR, A ,. «Estado constitucional de derecho, principios y derechos fundamentales en robert alexy». *Saber Ciencia y Libertad.* 2011, Vol. 1, pp. 6-7.

BARRIO, M,. « El cumplimiento basado en el riesgo o risk-bases compliance, pieza cardinal del nuevo Derecho digital europeo» . *Real Instituto elcano Royal Institute*. 2023, Vol. 51, p. 1.

COTE, L,. «Evaluación de impacto del tratamiento de datos personales en colombia y responsabilidad proactiva». *Superintendecia de Insdustria y comercio.* 2020. [en línea]. p. 9.

MORTIZ, M, GIBELLO V. 2021. El Reglamento Europeo (UE) 2016/679: análisis de un clarooscuro. *Revista de derecho UASB-E*. pp. 1-4.

RODRIGUEZ, D. 2019. *«Los Desafíos del Derecho de las TIC en la Sociedad de la Información en el Siglo XXI: Una Puerta a la Cooperación Internacional»*. España.

RALLO, A. *«* Hacia un nuevo sistema europeo de protección de datos: las claves de la reforma*»*. *Revista de Derecho Político (UNED)*. 2012, N.º 85. DOI 10.5944/rdp.85.2012.10244, pp.14-56. ISSN02119779X.

RODRIGUEZ,A. *«Los Desafíos del Derecho de las TIC en la Sociedad de la Información en el Siglo XXI: Una Puerta a la Cooperación Internacional»* España. 2019.

ESTEPA,M, 2022. «El principio de responsabilidad proactiva o rendición de cuentas como informador del régimen jurídico de la protección de datos de las personas físicas». *Anuario Jurídico y Económico Escurialense, LV* [en línea]. Vol. 55, p. 3. Disponible en : El principio de

responsabilidad proactiva o rendición de cuentas como informador del régimen jurídico de la protección de datos de las personas físicas - Dialnet (unirioja.es) [accedido 30 abril 2024].

FERNANDEZ, A, LLORENS, F. *Gobierno de las TI para universidades* «1968- y LLORENS, Faraón, 2011. *Gobierno de las TI para universidades* [en línea]. CRUE TIC. ISBN 9788493550981. Recuperado a partir de : https://tic.crue.org/wp-content/uploads/2016/04/gobierno_de_las_TI_para_universidades.pdf [accedido 3 mayo 2024].

MORALES, A. 2022. *IMPLEMENTANDO UN PROGRAMA DE CUMPLIMIENTO EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES* [en línea]. Perú. Recuperado a partir de : https://rpde.tytl.com.pe/wp-content/uploads/2022/11/06-IMPLEMENTANDO-UN PROGRAMA-DE-COMPLIANCE.pdf [accedido 1 mayo 2024].

RODRIGUEZ,A. *«Los Desafíos del Derecho de las TIC en la Sociedad de la Información en el Siglo XXI: Una Puerta a la Cooperación Internacional»* España. 2019.

SANTAMARIA, F. 2020. Vista de El principio de responsabilidad proactiva: una oportunidad para un mejor cumplimiento de la normativa en materia de protección de datos de carácter personal en el ámbito latinoamericano. *Revista de la facultad de Derecho PUCP* [en línea]. p. 8. Disponible en : Vista de El principio de responsabilidad proactiva: una oportunidad para un mejor cumplimiento de la normativa en materia de protección de datos de carácter personal en el ámbito latinoamericano (pucp.edu.pe) [accedido 1 mayo 2024].

TRUJILLO, C, FERNANDEZ, M y CABRERA, S. *PROTECCIÓN DE DATOS, RESPONSABILIDAD ACTIVA Y TÉCNICAS DE GARANTÍA CURSO DE «DELEGADO DE PROTECCIÓN DE DATOS» Adaptado a la nueva Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales María de los Ángeles Fernández Scagliusi*

Profesora Ayudante Doctora de Derecho Administrativo (Contratada Doctora acr.), Universidad de Sevilla Coordinadores. 2018.

VALERO, J , 2007. *El régimen jurídico de la e-Administración : el uso de medios informáticos y telemáticos en el procedimiento administrativo* [en línea]. Segunda. Granada : Comares. ISBN 9788498363104. Disponible en : https://www.comares.com/media/comares/files/book-attachment-6972.pdf [accedido 30 abril 2024].

SOLER, E 2020. Risk analysis and impact assessment relating to data protection: Its application to cooperative companies. *Boletin de la Asociacion Internacional de Derecho Cooperativo*. N.º 56, pp. 47-72. DOI 10.18543/BAIDC-56-2020PP47-72.

RODRIGUEZ, D. 2019. *«Los Desafíos del Derecho de las TIC en la Sociedad de la Información en el Siglo XXI: Una Puerta a la Cooperación Internacional»*. España.

ROMERO, I, 2020. Organizaciones sin delegado de protección de datos, en el punto de mira de la AEPD. *CincoDías*.

SIERRA, E 2018. *El delegado de protección de datos en la industria 4.0: funciones, competencias y las garantías esenciales de su estatuto jurídico*. . España.

Enlaces Web

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *« Gestión del riesgo y evaluación de impacto en tratamientos de datos personales»* [en línea]. 2021 [accedido 1 mayo 2024] Disponible en https://www.aepd.es/guias/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, *« Guía de Privacidad desde el Diseño»*[en línea].2019 [accedido 30 abril 2024] Disponible en: https://www.aepd.es/guias/guia-privacidad-desde-diseno.pdf

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, *« Guía de Protección de Datos por Defecto»*[en línea]. 2020 [accedido 3 junio 2024] Disponible en: https://www.aepd.es/guias/guia-proteccion-datos-por-defecto.pdf

CLUB LEGAL ASESORES INTERNACIONALES. RGPD – Unidad III : Accountability o Principio de Responsabilidad Proactiva. Disponible en: https://www.dpoitlaw.com/reglamento-general-de-proteccion-de-datos-rgpd/unidad-iii-1-2-2-accountability-privacidad-por-defecto-y-privacidad-por-diseno/

CORTIZAS DE CASTRO, Eladio, 2019. *Evaluación de Impacto relativa a la Protección de Datos* [en línea]. España : Interuniversitario UOC, UAB, URV, UIB. Disponible en : https://openaccess.uoc.edu/bitstream/10609/96626/15/ecortizasTFM0619memoria.pdf [accedido 1 mayo 2024].

GRUPO DE TRABAJO DE PROTECCIÓN DE DATOS DEL ARTÍCULO 29, 2010 *« Dictamen 3/2010 sobre el principio de responsabilidad»* [en línea]. Bruselas, Bélgica. Disponible en: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_es.pdf [accedido 1 mayo 2024].

GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29, 2017 « Directrices sobre la evaluación de impacto relativa a la protección de datos » [en línea]. Bruselas, Bélgica. Disponible en: wp248 rev.01_es (aepd.es).

GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29, 2017« Directrices sobre los delegados de protección de datos»[en línea]. Bruselas, Bélgica.Disponible en: wp248 rev.01_es (aepd.es).

GUILLEN, Andrea, 2017. *El Reglamento General de Protección de Datos y su impacto en las organizaciones: la figura del Delegado de Protección de Datos* [en línea]. España : UNIVERSIDAD DE LAS PALMAS DE GRAN CANARIA Facultad de Economía, Empresa y Turismo. Disponible:https://accedacris.ulpgc.es/bitstream/10553/22387/5/TFG%20FINAL%20Andrea Guill%c3%a9n.pdf [accedido 30 abril 2024].

INSTITUTO NACIONAL DE CYBERSEGURIDAD, 2015. *Gestión de riesgos- Una guia de aproximación para el empresario* [en línea]. España. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_gestion_riesgos_metad.pdf [accedido 5 mayo 2024].

Monzon,P. «Naturaleza la relación laboral de la protección de datos». *IUSLabor 2/2017* [en línea].2017. Disponible en : http://www.mjusticia.gob.es/cs/Satellite/Portal/1292428451504

PWC TAX&LEGAL SERVICES NEWSLETTER. *« Breves Regulación Digital: Sanciones entorno a la figura del Delegado de Protección de Datos Resolución de la Autoridad Belga».2020* accedido 5 junio 2024].Disponible en: https://periscopiofiscalylegal.pwc.es/wp-content/uploads/2020/06/Breves-Regulaci%C3%B3n-Digital-Sanciones-DPD-Junio-2020.pdf

Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the protection of individuals, 2012 [en línea].Disponible en : https://www.europarl.europa.eu/cmsdata/59702/att_20130508ATT65856-1873079025799224642.pdf

CORTIZAS DE CASTRO, Eladio, 2019. *Evaluación de Impacto relativa a la Protección de Datos* [en línea]. España : Interuniversitario UOC, UAB, URV, UIB. Disponible en: https://openaccess.uoc.edu/bitstream/10609/96626/15/ecortizasTFM0619memoria.pdf

[accedido 1 mayo 2024].

GUILLEN,A. 2017. *El Reglamento General de Protección de Datos y su impacto en las organizaciones: la figura del Delegado de Protección de Datos* [en línea]. España : UNIVERSIDAD DE LAS PALMAS DE GRAN CANARIA Facultad de Economía, Empresa y Turismo. Disponible en:

https://accedacris.ulpgc.es/bitstream/10553/22387/5/TFG%20FINAL%20AndreaGuill%c3%a9n.pdf [accedido 30 abril 2024].

SANTAMARIA, F, 2020. Vista de El principio de responsabilidad proactiva: una oportunidad para un mejor cumplimiento de la normativa en materia de protección de datos de carácter personal en el ámbito latinoamericano. *Revista de la facultad de Derecho PUCP* [en línea]. p. 8. Disponible en: https://revistas.pucp.edu.pe/index.php/derechopucp/article/view/22974/22001

[accedido 1 mayo 2024].

« Certificación de delegado de protección de datos*» aepd.* 5 de junio de 2020, Disponible en Certificación de Delegado de protección de datos | AEPD

Otros documentos

DOMINGUEZ, J , 2022. *UNIVERSIDAD DE SALAMANCA FACULTAD DE DERECHO* [en línea]. España : Facultad de derecho departamento de derecho administrativo, financiero y procesal programa de doctorado «administración,hacienda y justicia en el estado social». Disponible en: PDAHJES_DominguezAlvarezJL_Datos.pdf (usal.es) [accedido 30 abril 2024].

WILKINS, J, 2020. *Protección de datos por diseño y por defecto Principios fundacionales y marco normativo europeo Autor*. . Chile : Biblioteca del Congreso Nacional de Chile.

Legislación citada

Nacional

Ley Orgánica 3/2018, de 5 de diciembre, de protección de Datos Personales y garantía de los derechos digitales. *Boletín Oficial de Estado,* de 6 de diciembre de 2018, núm.294, pp.119788-119857.

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. *Boeltin Oficial del Estado,* de 14 de diciembre de 1999, núm. 298, pp. 43088-43099. (Derogada).

Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal*. Boletín Oficial del Estado***,** de 31 de octubre de 1992, núm.262, pp.3703-37045. (Derogada).

Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. *Boletin oficial del Estado*, de 19 de enero de 2008, núm. 17.

Internacional de la UE:

Reglamento (CE) n° 45/2001 del Parlamento Europeo y de Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las institucionaes y los organismos comunitarios y a la libre circulación de estos datos, de 12 de enero de 2001, serie L, núm. 8, pp.1-22 (Derogado).

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/ CE (Reglamento general de protección de datos), de 4 de mayo de 20146, serie L, núm.119,p.1.

Reglamento (UE) 2018/1725 del Parlemento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n°45/2001 y la Decisión n° 1247/2002(CE, de 21 de noviembre de 2018, serie L núm. 295, pp. 39-98.

Directiva 95/46/CE del Parlemento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. *Diario Oficial de las Comunidades Europeas*, 23 de noviembre de 1995, serie L, núm. 281, p.31. (Derogada).

CARTA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA. Diario Oficial de la Unión Europea, 18 de diciembre de 2020. Núm. 364/1. Disponible en: text_es.pdf (europa.eu)

TRATADO DE FUNCIONAMIENTO DE LA UNIÓN EUROPEA, de 13 de diciembre de 2007, versión consolidada (DOC 202 de 7.6.2016,pp. 47-360). Disponible en: Tratado de Funcionamiento de la Unión Europea | EUR-Lex (europa.eu).

Jurisprudencia referenciada

Sentencia del Tribuanal Supremo. Sala Tercera, de lo Contencioso-administrativo, sección 3°, Sentencia 188/2022 de 15 de febrero de 2022, Recurso N° 7359/2020 (Roj:STS 543/2022, ECLI: ES:TS: 2022:543). Disponible en: https://vlex.es/vid/897288138

Listado de abreviaturas

AEPD: Agencia Española de Protección de Datos

Art: Artículo

Arts: Artículos

CEPD: Comité Europeo de Protección de Datos

DPO: Data Protection Officer

DPD: Delegado de Protección de Datos

EIPD: Evaluación de Impacto de Protección de Datos

GT29: Grupo de Trabajo del artículo 29

OCDE: Organización de Cooperación y Desarrollo Económicos

PbD: Privacy by Desing

PDpD: Privacidad por defecto

PIA: *Privacy Impact Assessment*

UE: Unión Europea

ET: Encargado de Tratamiento

RT: Responsable de Tratamiento

ISO: Organización Internacional de Normalización

LOPDPGDD: Ley Orgánica de Datos Personales y Garantía de los Derechgos Digitales

PDCA: Planificar, Hacer, Verificar y Actuar

RGPD: Reglamento General de Protección de Datos

TFUE: Tratado de Funcionamiento de la Unión Europea

ENAC: Entidad Nacional de Acreditación

TFM: Trabajo fin de Master