Universidad Internacional de La Rioja
Máster Universitario en Propiedad Intelectual y Derecho de las Nuevas Tecnologías

La ciberseguridad como solución de privacidad: Especial incidencia en la privacidad desde el diseño

Trabajo de fin de máster presentado por: Roberto Gil Miñano

Titulación: Máster Universitario en Propiedad Intelectual y Derecho de las Nuevas Tecnologías

Área jurídica: Privacidad y protección de datos

Director: Don Juan Francisco Rodríguez Ayuso

Ciudad: Madrid

Fecha: 02 de febrero de 2020

Firmado por: Roberto Gil Miñano

ÍNDICE

I. RESUMEN

En un momento de la historia en el que la información es uno de los activos más importantes, ya no sólo de las empresas, sino de las personas, la protección de la misma se vuelve crucial para garantizar la privacidad de nuestro día a día. El mundo ha cambiado a una velocidad de vértigo y el entorno en el que vivimos ha pasado de físico a digital. Bajo este nuevo paradigma, en el que cada vez dependemos más de la tecnología y la usamos para generar ingentes cantidades de datos diarios, la única solución que nos permite arrojar algo de tranquilidad a nuestro nuevo estilo de vida es la ciberseguridad.

Por su lado, el mundo del Derecho, aunque más lentamente, también ha evolucionado. El legislador se ha actualizado a los nuevos tiempos y ha generado nuevas normas jurídicas que permiten instaurar unos mínimos legales para que las soluciones de ciberseguridad protejan nuestra información. Gracias a estas nueva legislación, se otorga un mayor control a los ciudadanos sobre su propia información, haciendo que el tratamiento de los datos de carácter personal adquiera un carácter transparente y confiable.

En este sentido, lo que en este trabajo se pretende es empezar identificando a los principales actores que participan en el ámbito de la protección de datos y desgranar los principios más importantes a los que han de atender para adecuar sus organizaciones a la legislación actual. A continuación, se profundizará en uno de los principales cambios que ha traído consigo el nuevo RGDP, un aspecto fundamental para todo aquel que pretenda desarrollar y comercializar servicios digitales de seguridad de la información, esto es, la protección de datos desde el diseño.

Palabras clave: “Reglamento General de Protección de Datos”, “Interesado”, “Responsable del Tratamiento”, “Protección de datos desde el diseño”, “Medidas técnicas y organizativas”.

ABSTRACT

At a time in history when information is one of the most important assets, not only of companies but also of individuals, its protection becomes crucial to ensure the privacy of our daily lives. The world has changed at a dizzying speed and the environment in which we live has gone from physical to digital. Under this new paradigm, in which we are increasingly dependent on technology and use it to generate huge amounts of data every day, the only solution that allows us to throw some peace of mind to our new lifestyle is cyber security.

The legal world, although slower, has also evolved. The legislator has adapted to the new times and has generated new legal rules that allow for the establishment of legal minimums for cybersecurity solutions to protect our information. Thanks to these new laws, citizens are given greater control over their own information, making the processing of personal data transparent and reliable.

In this sense, the main aim of this work is to identify the main actors involved in the field of data protection and to outline the most important principles to which they must adhere in order to bring their organizations into line with current legislation. It will then delve into one of the main changes brought about by the new GDPR, a fundamental aspect for all those who intend to develop and market digital information security services, that is, data protection by design.

Key words: "General Data Protection Regulation", "Data subject", "Data controller", "Data protection by design", "Technical and organisational measures".

II. LISTADO DE ABREVIATURAS Y SIGLAS

- AEPD: Agencia Española de Protección de Datos

- ET: Encargado del Tratamiento.

- Directiva 95/46: 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.

- LOPDGDD: Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

- RGPD: 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.

- RT: Responsable del tratamiento.

III. INTRODUCCIÓN: EL NUEVO PARADIGMA EN LA PROTECCIÓN DE DATOS

El RGPD es la mayor revisión de las normas de privacidad desde el nacimiento de Internet. En este nuevo contexto, el modelo de cumplimiento ha cambiado, pasando de un modelo de cumplimiento formal a un modelo de responsabilidad proactiva, en el que no incumplir ya no es suficiente, sino que ahora hay que cumplir y demostrarlo.

Más adelante entraremos en algunos ejemplos concretos, pero una correcta adecuación de las empresas al RGPD va a implicar necesariamente que sean capaces de garantizar la implementación de medidas tanto técnicas como otras propiamente jurídicas. [1]

En cuanto a las medidas técnicas, habrá que demostrar que se han hecho los análisis de riesgos pertinentes y que, en base a estos, se han ejecutado decisiones, tanto técnicas como organizativas[2], para crear diversas políticas internas en materia de privacidad, con obligaciones claras y acciones concretas, que permitan garantizar el cumplimiento de la norma.

En lo referente a las medidas jurídicas, los actuales RT deberán, entre otras, cumplir con las nuevas obligaciones de información a los interesados, determinar y justificar las bases jurídicas que sean adecuadas para recabar los datos que vayan a tratar, nombrar un delegado de protección de datos si cumplen determinadas condiciones y un largo etcétera de nuevas obligaciones que deberán atender, algunas de las cuales serán explicadas más adelante.

Todo esto es importante no sólo por el imperativo legal de su cumplimiento, sino porque el artículo 83 RGPD[3] contempla unas sanciones muy cuantiosas para aquellos

[1] "¿Qué es el Privacy by Design?". *Blog de protección de datos para empresas y autónomos – Grupo Ático 34*. 30 enero 2018. Disponible en: https://protecciondatos-lopd.com/empresas/privacy-by-design/
[2] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *El Reglamento de Protección de Datos en 12 preguntas* [en línea]. Disponible en: https://www.lopdat.es/noticias/el-reglamento-de-proteccion-de-datos-en-12-preguntas
[3] Artículo 83 "Condiciones generales para la imposición de multas administrativas" – RGPD. Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807

incumplimientos. Estas sanciones pueden ser (i) leves *(tales como infracciones de forma o respecto a obligaciones que no afecten a los interesados, por ejemplo la no designación de un DPO)* y ascender a 10.000.000 € como máximo o 2 % del volumen de negocio total anual global del ejercicio financiero anterior, la de mayor cuantía; o (ii) graves y muy graves *(P. ej. infracciones en las obligaciones de información, consentimiento, derechos o Transferencias Internacionales)* cuya cuantía puede llegar hasta los 20.000.000 € como máximo o 4 % del volumen de negocio total anual global del ejercicio financiero anterior, la de mayor cuantía.

En este sentido, es importante que las compañías conozcan qué papel juegan en este nuevo escenario y las obligaciones y responsabilidades asociadas al mismo. Para entender mejor esto, en el siguiente apartado describiremos los principales roles de esta norma.

1. La ciberseguridad y la protección de datos

Hoy tenemos a nuestra disposición más datos que nunca y novedosas maneras de gestionarlos y analizarlos para obtener conclusiones productivas para los negocios, y todo ello repercute no sólo en la cuenta de resultados de las empresas, sino en beneficios sociales en la vida de las personas. Por tanto, si los datos son el nuevo combustible de la economía, la protección de los mismos ha de ser nuestra nueva prioridad para alcanzar un clima estable de confianza.

Para evidenciar la relevancia actual de los datos tenemos declaraciones como las realizadas el 24 de mayo de 2018, un día antes de la entrada en vigor del RGPD, por el Vicepresidente de la Comisión Europea y Comisario europeo de Mercado Único Digital, Andrus Ansip, y por la Comisaria Europea de Justicia, Consumidores e Igualdad de Género, Věra Jourová. Andrus Ansip adelantaba que "*Two thirds of Europeans are concerned about the way their data was being handled, feeling they have no control over*

information they give online", mientras que Věra Jourová añadía que "*Personal data is the gold of the 21st century.*" y que "*Data protection is a fundamental right in the EU.*"[4]

A través de estas afirmaciones se pone en evidencia que los nuevos negocios ya son negocios de datos. Gracias a tecnologías como el *big data*, el internet de las cosas o el *cloud computing*, las barreras entre lo físico y lo digital están desapareciendo, de modo que los datos permiten conectar el mundo mediante nuevos productos y servicios.

Además, no podemos obviar que, en los últimos años, ha aumentado considerablemente la concienciación de la población respecto del valor y del poder que tiene la información que cada uno genera en su día a día.

En este nuevo modelo socioeconómico basado en los datos, el pilar esencial es la protección de los mismos, garantizando siempre un alto nivel de privacidad. Múltiples compañías de ciberseguridad han surgido en el mercado, prometiendo altos estándares de calidad a la hora de vender productos y servicios que gestionen y aseguran la información de sus clientes.

Todas estas empresas han de tener muy en cuenta la privacidad de los datos que van a tratar o jamás serán capaces de cultivar la confianza de los usuarios. Por tanto, hoy en día, cumplir con la normativa reguladora de la protección de datos no sólo es un imperativo legal, sino que ha de ser parte del ADN de las compañías de ciberseguridad.[5]

Estos elementos, ciberseguridad y protección de datos, son totalmente inseparables actualmente. El primero pretende garantizar la seguridad de todo tipo de información; el segundo va a sentar las bases jurídicas de cómo hacerlo para proteger

[4] "Statement by Vice-President Ansip and Commissioner Jourová ahead of the entry into application of the General Data Protection Regulation". *European Commission oficial website*. 24 de mayo de 2018. Disponible en: https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_18_3889

[5] GARCÍA HERRERO, J. *Privacidad desde el Diseño o "Privacy by Design" en el Reglamento General de Protección de Datos (I)* [en línea]. 08 de noviembre de 2016. Disponible en: https://jorgegarciaherrero.com/privacidad-desde-el-diseno-o-privacy-by-design-i/

aquella parte de la información que es personal y propia de los interesados. Por tanto, cualquier empresa que se dedique a lo primero ha de interiorizar e implantar unos principios que les permita garantizar la inviolabilidad de los datos que pretende proteger.

Para ello, a continuación realizaremos un primer acercamiento al marco normativo al que toda empresa de ciberseguridad se ha de adherir, a los principales cambios con los que han debido aprender a convivir estas compañías en los últimos tres años desde que entró en vigor el Reglamento Europeo de Protección de Datos, así como a los roles que las empresas pueden adquirir y profundizaremos en una de las ideas más importantes que toda empresa que desarrolle productos destinados a la seguridad de la información ha de interiorizar: la privacidad desde el diseño.

2. Marco normativo

Reconociendo la importancia del origen de la normativa actual, haremos un sucinto repaso por el camino legislativo que nos ha llevado a la actual regulación en materia de protección de datos.

Desde que el 29 de diciembre de 1978 entrara en vigor la actual Constitución Española[6], su artículo 18.4[7], que reza "*La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos*", ha sido la base sobre la que se han ido desarrollando diversas disposiciones legales de diferente rango que han permitido regular el impacto de la privacidad en los ciudadanos.

Antes de entrar a mencionar las diferentes normas que han regulado esta materia en nuestro país, es interesante prestar atención a cómo el propio Tribunal Constitucional ha venido fijando Doctrina a través de la cual puede observarse la

[6] Constitución Española. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-1978-31229
[7] Artículo 18 "Constitución Española". Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-1978-31229

evolución de la protección de datos personales. Así, por ejemplo, en su Sentencia 254/1993, de 20 de julio, se pronunciaba ligeramente sobre el derecho de acceso, aclarando levemente que cada sujeto debe poder acceder a sus propios datos[8]. Años más adelante, en el 2000 concretamente, encontramos otras Sentencias del Tribunal Constitucional que ya hacen referencia a la protección de datos como un derecho fundamental, dejando de este modo atrás el concepto que se venía teniendo de autodeterminación informativa. Así por ejemplo, la Sentencia 290/2000, de 30 de noviembre, considera derecho fundamental que los españoles puedan ejercer potestades respecto a ficheros que contengan sus datos personales[9].

De este modo, en España hemos convivido con distintas Leyes Orgánicas *(y con sus respectivos Reales Decretos que las desarrollaban)* que legislaban sobre esta materia.

El primer ejemplar de estas leyes lo encontramos en la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen[10], que estuvo vigente durante aproximadamente una década hasta que fue derogada por la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal[11], conocida como LORTAD.

En 1995 se adoptó en la Unión Europea la Directiva 95/46[12], la cual legislaba sobre el tratamiento de datos personales dentro del territorio de la Unión Europea, tratando de garantizar la libre circulación de datos y las garantías de su protección cuando se produjesen transferencias internacionales. De acuerdo con el Tratado de Funcionamiento de la Unión Europea, concretamente su artículo 288 (antiguo artículo

[8] Sentencia de 20 de julio de 1993, STC 254/1993, ECLI:ES:TC:1993:254. Disponible en: http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/2383#complete_resolucion&completa

[9] Sentencia de 30 de noviembre de 2000, STC 290/2000, ECLI:ES:TC:2000:290 Disponible en: http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/4274#extractos

[10] Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-1982-11196

[11] Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-1992-24189

[12] 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 respeta al tratamiento de datos personales y a la libre circulación de estos datos. Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-1995-81678

249 TCE), "l*a directiva obligará al Estado miembro destinatario en cuanto al resultado que deba conseguirse, dejando, sin embargo, a las autoridades nacionales la elección de la forma y de los medios."*[13]. Esto implica que, al tratarse de una Directiva, esta no era directamente aplicable, sino que necesitaba una norma nacional que la traspusiera al derecho nacional español.

De este modo, la LORTAD fue derogada y sustituida por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal[14], que traspuso a nuestro derecho la anteriormente mentada Directiva y que, junto con el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprobó el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal[15], ha estado en vigor durante aproximadamente 20 años, siendo la norma de protección de datos con la que más tiempo hemos convivido en España.

Continuando con el orden cronológico, pero trasladándonos ahora al ámbito europeo, el 25 de enero de 2012 la Comisión Europea presentó al Parlamento Europeo y al Consejo una primera propuesta de Reglamento General de Protección de Datos[16]. Tras varios años, el 4 de mayo de 2016, el RGPD[17] fue publicado en el Diario Oficial de la Unión Europea, entrando en vigor veinte días después de esta publicación, es decir, el 24 de mayo de 2016 y, según indica su artículo 99, sería aplicable a todos los Estados

[13] Artículo 288 "Tratado de la Unión Europea y del Tratado de Funcionamiento de la Unión Europea. Versiones consolidadas. Protocolos. Anexos. Declaraciones anejas al Acta Final de la Conferencia intergubernamental que ha adoptado el Tratado de Lisboa". Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-Z-2010-70002

[14] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-1999-23750

[15] 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. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2008-979

[16] COUNCIL OF THE EUROPEAN UNION. *Proposal for a 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)*. 27 de enero de 2012. Disponible en: http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%205853%202012%20INIT

[17] 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). Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807

Miembros a partir del 25 de mayo de 2018[18], fecha a partir de la cual quedaría igualmente derogada la Directiva 95/46, de acuerdo con lo estipulado en su artículo 94.1[19].

Es fundamental mencionar aquí las implicaciones del cambio que supuso para la Unión Europea pasar de una Directiva a un Reglamento. En la Unión Europea se dictan diferentes disposiciones legislativas. De este modo, el Consejo y la Comisión Europea pueden adoptar, entre otros, Reglamentos y Directivas. Aunque ambas normas son vinculantes, los Reglamentos son enteramente obligatorios y directamente aplicables en cada Estado Miembro[20], mientras que la Directiva indica el resultado final al que cada Estado Miembro ha de llegar, pero les deja libertad para elegir la forma y los medios, es decir, necesita de una norma local para ser de efectivo cumplimiento.

Por tanto, el marco jurídico europeo pasó de estar sustentado por la Directiva 95/46 a estarlo por el RGPD. Analicemos bien el cambio, anteriormente se requería que cada Estado miembro legislara internamente la manera en la que iba a cumplir con las obligaciones que esta Directiva imponía, lo que suponía que los países integrantes de la Unión Europea tenían libertad para trasladar esta norma. Esto trajo consigo una desigualdad entre las legislaciones de cada país, lo que dificultaba las negociaciones que implicaban tratamientos en distintos países. No podemos sino mentar aquí el tercer expositivo del preámbulo del RGPD, que define magistralmente la heterogeneidad que reinó en Europa al respecto: "*La transposición de la directiva por los Estados miembros se ha plasmado en un mosaico normativo con perfiles irregulares en el conjunto de la Unión Europea lo que, en último extremo, ha conducido a que existan diferencias apreciables en la protección de los derechos de los ciudadanos.*"[21]

[18] Artículo 99 "Entrada en vigor y aplicación" – RGPD. Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807

[19] Artículo 94 "Derogación de la Directiva 95/46/CE" – RGPD. Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807

[20] Artículo 288 "Tratado de la Unión Europea y del Tratado de Funcionamiento de la Unión Europea. Versiones consolidadas. Protocolos. Anexos. Declaraciones anejas al Acta Final de la Conferencia intergubernamental que ha adoptado el Tratado de Lisboa". Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-Z-2010-70002

[21] Expositivo III del Preámbulo RGPD. Disponible en: https://www.boe.es/boe/dias/2018/12/06/pdfs/BOE-A-2018-16673.pdf

Sin embargo, en la actualidad, el RGPD ha supuesto que, de repente, todos los países integrantes de la Unión Europea estén regulados bajo un mismo paraguas normativo y, lo que es más importante, una garantía para los ciudadanos por cuanto en todo el territorio Europeo sus datos van a ser tratados en igualdad de condiciones. Es cierto que cada país ha debido adaptar su ordenamiento a dicho reglamento, pero los principios que rigen el tratamiento de datos de los ciudadanos europeos por parte de toda entidad, pública o privada, se rigen ahora por idénticos principios.

Es decir, con el RGPD, la Unión Europea no solo pretende actualizar la regulación existente en ese momento, sino que busca revisar el modelo legislativo que regula la privacidad de sus ciudadanos, y armonizarlo, dado que hasta el momento actual esta era bien diferente en cada estado miembro. De este modo, se genera una seguridad jurídica trasversal para todos los Estados miembros, pero sin excluir a los poderes legislativos de cada país, obligando a que cada derecho nacional integre clara y transparentemente las bases legales de esta nueva regulación europea, obligándole igualmente a eliminar toda aquella normativa que pudiera resultar incompatible.

Volviendo a las normas que se han aplicado en cada momento en España, nos encontramos que tras la entrada en vigor del RGPD, nos hallamos con un periodo transitorio (*desde el 24 de mayo de 2016 hasta el 25 de mayo de 2018*) en el que en España seguían siendo de aplicación tanto la Directiva 95/46, como las normas nacionales de desarrollo anteriormente mencionadas[22]. No obstante, durante estos 2 años, las empresas iban a gozar de un plazo limitado de tiempo durante el cual debían empezar a prepararse y adoptar las nuevas medidas exigidas para cumplir, a partir del 25 de mayo de 2018, con las previsiones del RGPD.[23]

[22] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *El Reglamento de Protección de Datos en 12 preguntas* [en línea]. Disponible en: https://www.lopdat.es/noticias/el-reglamento-de-proteccion-de-datos-en-12-preguntas

[23] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Guía del Reglamento General de Protección de Datos para responsables de tratamiento* [en línea]. Disponible en: https://www.aepd.es/sites/default/files/2019-09/guia-rgpd-para-responsables-de-tratamiento.pdf

Una vez llega el 25 de mayo de 2018, fecha a partir de la cual la Directiva 95/46 es derogada y el RGPD es de plena aplicación, España aún no contaba con una Ley propia que incorporase al derecho español la regulación europea, que llegaría en diciembre del mismo año, por lo que para esos 6 meses (*desde 25 de mayo de 2018 hasta 05 de diciembre de 2018*) fue necesario aprobar el Real Decreto-ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos[24], cuyo objetivo fue, como resalta su exposición de motivos "*la adecuación de nuestro ordenamiento al reglamento europeo en aquellos aspectos concretos que, sin rango orgánico, no admiten demora […]*". Concretamente, este Real Decreto-ley 5/2018, de 27 de julio, derogado posteriormente por la LOPDGDD, se encargó de regular, como igualmente identifica su exposición de motivos, (i) la actividad de investigación e inspección, (ii) el novedoso régimen sancionador y (iii) el procedimiento en caso de que exista una posible vulneración del Reglamento General de Protección de Datos.

Finalmente, llegamos al mes de diciembre de 2018, momento en el que se aprueba la actual Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales[25] (en adelante, "LOPDGDD"), por la que se deroga tanto el Real Decreto-ley 5/2018, de 27 de julio, como la Ley Orgánica 15/1999 (salvo sus artículos 23 y 24, que continúan en vigor en tanto no sean expresamente modificados, sustituidos o derogados).

Por tanto, actualmente, el marco normativo español en cuanto a protección de datos está configurado por el RGPD y la LOPDGDD, que no desarrolla el RGDP, sino que incorpora al derecho español la regulación del RGPD y, en aquello que sea necesario, lo completa.

[24] Real Decreto-ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-2018-10751

[25] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673&p=20190625&tn=6

Otras normas que denotan la relevancia que está adquiriendo esta materia para los legisladores son:

- DIRECTIVA (UE) 2016/680 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo[26].

- DIRECTIVA (UE) 2016/1148 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión27 (Conocida como la Directiva NIS).

- En camino una propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas)[28].

Sin ánimo de entrar a valorar estas disposiciones, es nuestra intención al mencionarlas resaltar la preocupación existente en la actualidad por regular

[26] DIRECTIVA (UE) 2016/680 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo. Disponible en: https://www.boe.es/doue/2016/119/L00089-00131.pdf

[27] DIRECTIVA (UE) 2016/1148 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. Disponible en: https://www.boe.es/doue/2016/194/L00001-00030.pdf

[28] Propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas). Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52017PC0010

adecuadamente un marco normativo que permita proteger la privacidad de los individuos en distintas materias de nuestro día a día, al igual que nos permite observar cómo la regulación de la protección de datos no ha sido ni mucho menos estática, sino que el ritmo evolutivo que ha marcado la tecnología ha llevado a los diferentes legisladores a un proceso dinámico y, sobre todo, internacional. Los avances tecnológicos que mencionamos permiten un cada vez mayor flujo internacional de datos que ha transformado nuestra vida social y económica, por lo que ya no basta con normativas nacionales, sino que son necesarias reglas trasversales que permitan homogeneizar la regulación del dato en todo el mundo[29].

Conociendo esto, podemos iniciar el análisis de los principales puntos que aquí queremos resaltar.

IV. LOS PROTAGONISTAS PRINCIPALES DE LA NUEVA NORMATIVA

Aunque el RGPD trae consigo nuevos términos, algunos ya los conocíamos de a regulación legislativa anterior, pero conviene destacar tres de estos términos, pues son los que nos van a permitir conocer a los principales actores de los derechos y obligaciones en los que más adelante nos centraremos.

1. El Interesado

Debemos acudir al artículo 4 RGPD[30] para encontrar, en su punto primero, la siguiente definición "*«datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos*

[29] FUERTES NIETO, M. Informe sobre la vulneración de los derechos al Honor, Imagen y privacidad en el ámbito médico por uso de tecnología. Tutor: Fernando Fonseca Ferrandis. Universidad Carlos III de Madrid, Departamento de Derecho, Madrid, 2019.

[30] Artículo 4 "Definiciones" – RGPD. Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807

propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;".

Indicar, sin entrar a evaluar en detalle, que la redacción original del RGPD utiliza la expresión "*data subject"*[31] para identificar al sujeto titular de los datos. En la redacción en castellano no debemos confundir nuestro "Interesado" *(titular de los datos)* con aquellos otros interesados en los propios datos como puedan ser las administraciones públicas o las empresas privadas.

Podemos entonces concluir que el Interesado será la persona física titular de los datos que son objeto del tratamiento por parte de los responsables y encargados del tratamiento, como vienen definidos más adelante.

Cualquier compañía que ofrezca y/o venda productos y servicios de ciberseguridad y que, por tanto, lleve a cabo tratamiento de datos bien como responsable o encargado, habrá de ser capaz de garantizar los derechos que se reconocen a todo Interesado al amparo de los artículos 15 a 22 del nuevo RGPD, y sus correspondientes en la LOPDGDD. [32]

Muy resumidamente, y sin profundizar en el alcance, ni en las obligaciones del RT ante el ejercicio de tales derechos del Interesado, estos serían:

- Derecho de acceso: El Interesado tiene derecho a que quien esté realizando un tratamiento sobre sus datos personales le facilite una copia de estos. Este derecho viene recogido en el artículo 15 RGPD y 13 LOPDGDD.

[31] Article 4 "Definitions" - REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

[32] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Protección de Datos: Guía para el Ciudadano* [en línea]. Disponible en: https://www.aepd.es/sites/default/files/2019-10/guia-ciudadano.pdf

- Derecho de rectificación: El Interesado tiene derecho a rectificar aquellos datos personales inexactos o erróneos que se estén tratando sobre él, así como a completar datos incompletos. Este derecho viene recogido en el artículo 16 RGPD y 14 LOPDGDD.

- Derecho de supresión ("el derecho al olvido"): El Interesado tiene derecho a que sean suprimidos los datos personales que le conciernan cuando (i) los datos ya no son necesarios; (ii) retira su consentimiento o se opone y no existe otra base legitimadora; (iii) son tratados ilícitamente; y (iv) existe una obligación legal de supresión. Este derecho viene recogido en el artículo 17 RGPD y 15, 93 y 94 LOPDGDD.

- Derecho a la limitación del tratamiento: El Interesado tiene derecho a que se limite el tratamiento de sus datos personales cuando (i) impugne la exactitud de los mismos; (ii) el tratamiento sea ilícito pero el propio Interesado se oponga a la supresión de los datos; (iii) los datos ya no sean necesarios para el fin para el que se recabaron; y (iv) el Interesado se haya opuesto al tratamiento pero aún sean necesarios para verificar los motivos de esta oposición. Este derecho viene recogido en el artículo 18 RGPD y 16 LOPDGDD.

- Derecho a la portabilidad de los datos: El Interesado tiene derecho a recibir los datos en un formato interoperable y a solicitar la transmisión de los datos a otro RT. Este derecho viene recogido en el artículo 20 RGPD y 17 LOPDGDD.

- Derecho de oposición: El Interesado tiene derecho a poder oponerse a que los datos sean objeto de un tratamiento cuando la base legitimadora sea interés legítimo Este derecho viene recogido en el artículo 21 RGPD y 18 LOPDGDD.

- Derecho de oposición a decisiones automatizadas: El Interesado tiene derecho a exigir no ser objeto de decisiones basadas únicamente en tratamientos automatizados *(elaboración de perfiles, entre otros)*, que produzca sobre el propio Interesados efectos jurídicos. Este derecho viene recogido en el artículo 22 RGPD[33].

[33] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Protección de Datos: Guía para el Ciudadano* [en línea]. Disponible en: https://www.aepd.es/sites/default/files/2019-10/guia-ciudadano.pdf

2. El responsable del tratamiento

Acudimos al artículo 4 RGPD[34] para conocer a este protagonista e identificarlo como el RT, al que se define como "*la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento*".

De lo anterior se desprende que la clave para definir este rol es que el RT es quien determina los fines y medios del tratamiento, es decir, será quien establezca la finalidad para la cual se van a utilizar los datos personales del interesado y, por ende, sobre el que recaen la mayoría de las obligaciones del RGPD.[35]

La principal de estas obligaciones es asegurarse de que el tratamiento que va a llevar a cabo está permitido al amparo de la regulación actual. En este sentido, la licitud o ilicitud de un tratamiento vendrá determinada por el cumplimiento o no, respectivamente, de los principios relativos al tratamiento de datos personales que vienen recogidos en el artículo 5 del RGPD[36], siendo este uno de los artículos más importantes de la norma, si no el que más. Es por ello que estos principios son el fundamento del nuevo sistema legislativo de protección de datos de carácter personal. Sí es cierto que algunos de ellos vienen heredados de la Directiva 95/46, pero el RGPD ha sabido recoger la relevancia de los mismos e incluso los ha dotado de una descripción más actual que permiten tenerlos mejor identificados por los propios RT.

[34] Artículo 4 "Definiciones" – RGPD. Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807

[35] LEFEBVRE, F. *Memento Práctico Protección de Datos*. Editorial Jurídica Lefebvre®, 2019. ISBN 978-84-17544-49-2.

[36] Artículo 5 "Principios relativos al tratamiento" – RGPD. Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807

El artículo 5 encuentra su referencia en el considerando 39 del RGPD[37], al que podemos acudir para entender correctamente alguno de los principios que aquí se recogen. Concretamente, los principios aplicables que todo RT ha de cumplir son[38]:

- Principio de licitud, lealtad y transparencia [art.5.1.a) RGPD]: La licitud del tratamiento se refiere a que el mismo esté amparado por algunas de las bases legitimadores que se establecen en el artículo 6 del RGDP. Esto es, los datos no pueden simplemente tratarse porque uno tenga acceso a ellos, sino que podrán ser tratados cuando exista un amparo legal para ello.

  En cuanto a la lealtad, este principio impide que los datos sean tratados de una forma desleal o confusa para con el interesado.

  Por último, la transparencia requiere que el interesado sea plenamente consciente de quien está tratando sus datos de carácter personal, así como las razones de para qué se está haciendo y el modo en el que se está haciendo. Toda esta información habrá de ser comunicada de manera clara y sencilla.

- Principio de limitación de la finalidad [art.5.1.b) RGPD]: Únicamente resaltar aquí los adjetivos que recoge el propio RGPD aplicables a la finalidad para la que pueden ser tratados los datos, a saber, "*determinados, explícitos y legítimos*". Esta finalidad ha de ser determinada antes de tratar estos datos y, en todo caso, habrá de ser trasladada explícitamente al interesado para que sea consciente de la razón por la cual se tratan sus datos, que ha de ser legítima, es decir, no debe contravenir con la ley o el derecho.

[37] Considerando 39 RGPD. Disponible en: https://www.boe.es/doue/2016/119/L00001-00088.pdf

[38] INSTITUTO NACIONAL DE ADMINISTRACIÓN PÚBLICA. MINISTERIO DE HACIENCIA Y ADMINISTRACIONES PÚBLICAS. *El Reglamento General de Protección de Datos. Módulo 1: Marco general para el tratamiento de datos personales* [en línea]. Disponible en: https://www3.gobiernodecanarias.org/cpji/gestionconocimiento/_recursos/proteccion_datos/resources/Modulo_1.pdf

- Principio de minimización de datos [art.5.1.c) RGPD]: Este principio viene a obligar a recabar y tratar, exclusivamente, aquellos datos que sean "*adecuados, pertinentes y limitados*" a lo realmente necesario a los fines para los cuales han sido recogidos[39]. Este principio es fundamental para el cumplimiento de las obligaciones relativas a la privacidad desde el diseño que más adelante entraremos a analizar.

- Principio de exactitud [art.5.1.d) RGPD]: Este principio se comprende mejor acudiendo, como decíamos anteriormente, al Considerando 39, en el que se nos indica que "*Deben tomarse todas las medidas razonables para garantizar que se rectifiquen o supriman los datos personales que sean inexactos*.". Es decir, los datos han de ser precisos para evitar las posibles consecuencias que podrían llegar a sufrir aquellos interesados sobre los que se tratasen datos inexactos sobre ellos.

- Principio de limitación del plazo de conservación [art.5.1.e) RGPD]: Este principio está íntimamente ligado al de minimización, siendo otro de los principios fundamentales que más interesa a la privacidad desde el diseño. Lo que aquí el RGPD obliga es a retener y tratar los datos sólo durante el tiempo estrictamente necesario para cumplir con la finalidad para que fueron recabados, obligando al RT a suprimir los datos en cuanto estos dejen de ser necesarios. Es decir, el RT no puede conservar los datos una vez la finalidad ha sido cubierta.

- Principio de integridad y confidencialidad [art.5.1.f) RGPD]: Con este principio, el legislador europeo pretende obligar al RT a tener implementadas una serie de medidas adecuadas y razonables que le permiten garantizar la integridad y la confidencialidad de los datos de carácter personal que trata, previniendo la posible fuga de estos datos. Cabe mencionar que este es un principio que no venía recogido en la Directiva, por lo que ha nacido con el RGPD.

[39] CHINEA LÓPEZ, J. *La privacidad desde el diseño. ¿Por legalidad o responsabilidad?* [en línea]. 26 de diciembre de 2012. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/privacidad-desde-diseno

- Principio de responsabilidad proactiva (art.5.2. y 24 RGPD): La responsabilidad proactiva (o accountability, según su extendida acepción inglesa) es la mayor novedad que trae consigo el RGPD, al menos en cuanto a las obligaciones de los RT. Viene introducido en el Considerando 85, presentado como obligación en el artículo 5.2 y desarrollado en el 24.

  Con este principio, dejamos atrás un modelo en el que era suficiente con cumplir con las obligaciones que imponían las disposiciones legales en materia de protección de datos, para pasar a otro modelo en el que ahora el RT ya no solo es responsable de ese cumplimiento, sino que ahora, además, ha de ser capaz de demostrarlo. Para poder demostrarlo, el RT deberá buscar qué medidas técnicas y organizativas necesita implementar para garantizar el cumplimiento de este principio.

  En términos prácticos, este principio requiere que las organizaciones analicen qué datos tratan, con qué finalidades lo hacen y qué tipo de operaciones de tratamiento llevan a cabo. A partir de este conocimiento deben determinar de forma explícita la forma en que aplicarán las medidas que el RGPD prevé, asegurándose que esas medidas sean las adecuadas para cumplir con el mismo y que puedan demostrarlo ante los interesados y ante las autoridades de supervisión[40].

  En síntesis, este principio exige una actitud consciente, diligente y proactiva [41]por parte de las organizaciones frente a todos los tratamientos de datos personales que lleven a cabo[42].

[40] LEFEBVRE, F. *Memento Práctico Protección de Datos*. Editorial Jurídica Lefebvre®, 2019. ISBN 978-84-17544-49-2.
[41] ALIÑO SEHWERERT, J.J. *Cómo implementar el Reglamento General de Protección de Datos en la empresa*. Abril 2018
[42] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Guía del Reglamento General de Protección de Datos para responsables de tratamiento* [en línea]. Disponible en: https://www.aepd.es/sites/default/files/2019-09/guia-rgpd-para-responsables-de-tratamiento.pdf

> Probablemente, una de las medidas más relevantes para que un RT pueda cumplir con su responsabilidad proactiva sea la que ocupa este trabajo, es decir, la aplicación de la protección de datos desde el diseño.[43]

Como es lógico, no todos estos principios tienen la misma relevancia de cara al tema que aquí nos ocupa, pero es innegable que algunos de ellos han ejercido una gran influencia en la filosofía de la privacidad desde el diseño y son esenciales a la hora de implementar correctamente la privacidad desde el diseño de un producto, como pueden ser los principios de (i) licitud, lealtad y transparencia; (ii) minimización; (iii) limitación del plazo de conservación; y (iv) responsabilidad proactiva.

Como venimos diciendo, todo RT ha de tomar las medidas necesarias que le permitan garantizar ante cualquier interesado el cumplimiento de estos principios a la hora de tratar sus datos de carácter personal. Conviene resaltar la obligación que tiene todo RT de informar al interesado sobre el tratamiento que va a hacer de sus datos personales. Este deber de información se materializa en lo que conocemos como "política de privacidad". En la misma, el RT ha de informar sobre (i) quién es el RT; (ii) qué datos personales son objeto del tratamiento; (iii) cómo se recogen y cuál es la procedencia de los datos; (iv) para qué y porqué se tratan los datos; (v) durante cuánto tiempo se conservan los datos; (vi) quién tiene acceso a los datos y si hay transferencias internacionales *(salida de datos a países fuera de la Unión Europea)*; (vii) cuáles son los derechos del Interesado y como pueden ejercitarse; (viii) qué salvaguardas y medidas de seguridad se aplican; y (ix) qué aspectos más importantes se deben tener en cuenta.

Aunque muy brevemente, es importante aquí mencionar que no es lo mismo que un interesado acepte una política de privacidad a que otorgue su consentimiento para el tratamiento, pues la política de privacidad cumple una función informativa (de acuerdo con los artículos 13 y 14 RGPD y 11 LOPDGDD), mientras que el consentimiento es una base legitimadora de un tratamiento específico (artículos 6 y 7 RGPD y artículos

[43] LEFEBVRE, F. *Memento Práctico Protección de Datos*. Editorial Jurídica Lefebvre®, 2019. ISBN 978-84-17544-49-2.

6, 7 y 8 LOPDGDD[44]). Todo RT debe tener muy en cuenta que el consentimiento no puede considerarse incluido dentro de la política de privacidad.

Para terminar, no debemos olvidar que todas estas medidas no sólo son de obligatoria aplicación por parte de los RT, sino también por los ET, figura que pasamos a analizar a continuación.

3. El encargado del tratamiento

Al igual que en los apartados anteriores, debemos acudir al artículo 4 RGPD[45] para conocer la definición que se recoge en la norma sobre el ET, al que se identifica como "*la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento*".

Es conveniente tener claro que las empresas pueden tratar los datos por sí mismas o a través de terceras partes, bien sean personas físicas o jurídicas. Estos terceros a los que un RT puede acudir para solicitar la prestación de determinados servicios, que lleven aparejados el acceso y el tratamiento de datos de carácter personal, son los que conocemos como ET.

Cuando un RT decide encomendar el tratamiento de datos personales a un tercero, el primero ha de asegurarse de que el segundo ofrece unas garantías suficientes de cumplimiento del RGPD[46]. Por tanto, los ET han de ser capaces de demostrar que poseen unas medidas técnicas y organizativas suficientes para garantizar la privacidad de los interesados, y que estas medidas serán proporcionadas en todo momento[47].

---

[44] SEMPERE, FJ. *Crossover entre el RGPD y la nueva LOPD* [en línea]. 13 de diciembre de 2018. Disponible en: http://www.privacidadlogica.es/crossover-entre-el-rgpd-y-la-nueva-lopd/

[45] Artículo 4 "Definiciones" – RGPD. Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807

[46] PUYOL MONTERO, J. *Pautas para la implantación del RGPD: Las relaciones entre el responsable y el encargado del tratamiento. El tratamiento de datos por terceros. Los contratos de prestación de servicios y las nuevas exigencias de la contratación*. Mayo 2018

[47] LEFEBVRE, F. *Memento Práctico Protección de Datos*. Editorial Jurídica Lefebvre®, 2019. ISBN 978-84-17544-49-2.

El concepto esencial que necesitamos entender es que un ET no decide sobre el tratamiento ni establece la finalidad para la cual se produce el mismo, sino que siempre trata los datos personales por cuenta del RT, es decir, siguiendo siempre sus instrucciones. Si esto no fuera así, es decir, si el ET estuviera tratando los datos de carácter personal, a los que ha accedido gracias al RT para su propia finalidad, dejaría de ser ET para convertirse en otro RT más.

Para regular estas instrucciones, entre RT y ET, debe suscribirse un acuerdo de tratamientos de datos con un contenido determinado, que viene regulado en los artículos 28 RGPD y 33 LOPDGDD[48].

Igualmente, todo ET debe asistir al RT en el cumplimiento del RGPD y cooperar para el ejercicio de derechos y aplicar medidas de seguridad. Igualmente, un ET puede a su vez encargar el tratamiento a otra empresa, la cual tendrá la consideración de Subencargado del Tratamiento, siempre que cuente con la autorización del RT.

V. PRIVACIDAD DESDE EL DISEÑO

1. Concepto, origen y principios

a. Concepto

Irremediablemente debemos comenzar esta sección explicando el concepto de "Privacidad desde el diseño" o "Protección de datos desde el diseño". El problema es que no existe una definición clara como las que podemos encontrar en el artículo 4 del RGPD, pues históricamente ha sido un concepto abstracto que hasta la entrada en vigor del RGPD ni siquiera venía expresamente en los textos legales. Se trata más bien de una filosofía, de un enfoque proactivo de la privacidad, de una exigencia en la manera de actuar, pero la falta de concreción respecto a cómo implementar dentro de una

[48] SEMPERE, FJ. *Crossover entre el RGPD y la nueva LOPD* [en línea]. 13 de diciembre de 2018. Disponible en: http://www.privacidadlogica.es/crossover-entre-el-rgpd-y-la-nueva-lopd/

compañía esta filosofía, este enfoque o estas exigencias, ha hecho que se trate más bien de un concepto holístico que de una realidad tangible. [49]

Lo que la normativa pretende con este concepto es obligar, tanto a empresas que diseñan tecnologías que permiten el acceso, el tratamiento y la comunicación de información, como a aquellas otras empresas que comercializan o emplean estas tecnologías como parte de su actividad diaria, a que incluyan, bien desde que empiezan a diseñar o desarrollar estas tecnologías o desde que las implementan en sus propias compañías o en compañías de terceros, las medidas técnicas y/u organizativas necesarias para velar correctamente por la privacidad de los usuarios finales[50]. Esto sólo será posible si las empresas tienen interiorizada una filosofía claramente defensora de las normas de protección de datos. Gracias a esta visión preventiva, las compañías que apliquen este principio serán capaces de limitar los posibles riesgos que en el futuro se puedan originar en cuanto a los tratamiento de datos que lleven a cabo.

Este concepto pretende integrar la privacidad tanto en los sistemas tecnológicos que permiten llevar a cabo un tratamiento de datos personales como en las propias organizaciones que llevan a cabo estos tratamientos, de tal manera que se puedan reducir al mínimo las probabilidades de ocurrencia de cualquier incidente que pueda afectar a la privacidad del usuario. Por tanto, una empresa que llegue a cumplir efectivamente con este enfoque estaría "incrustando" la protección de datos dentro del diseño de la tecnología.[51]

Como decíamos, hasta 2018 no había sido un imperativo legal, pero desde entonces todo obligado por la norma pasa a estar igualmente sujeto a sanciones sustanciales en caso de violar este principio como explicaremos más adelante. El

[49] VEALE, M., BINNS, R., AUSLOOS, J. "When data protection by design and data subject rights clash". International Data Privacy Law. 2018. Vol. 8. No. 2. [consulta: diciembre de 2018]. doi:10.1093/idpl/ipy002. Disponible en: https://academic.oup.com/idpl/article-pdf/8/2/105/25113376/ipy002.pdf

[50] PUYOL MONTERO, J. *La privacidad responsable o la privacidad por el diseño*. Junio 2017

[51] *Complylaw Privacidad | Privacidad desde el diseño: Enfoque práctico y medidas a adoptar*. Wolters Kluwer España. 20 de septiembre de 2019. Youtube. Disponible en: https://www.youtube.com/watch?v=yU7OgqIeY2w

problema es que no queda claramente definido cómo se debe cumplimentar esta exigencia.

b. Origen

Tal vez la manera más acertada de acercarnos a este principio sea acudir a los orígenes del mismo. Para ello, debemos remontarnos a los años 90, momento en el que la Doctora Ann Cavoukian desarrolló e introdujo por primera vez la privacidad por diseño, definiéndolo como "*la filosofía y el enfoque de integrar la privacidad en las especificaciones de diseño de diversas tecnologías*[52]".

Este nuevo concepto de privacidad fue necesario debido a los crecientes derechos que venían otorgándose a los ciudadanos en materia de privacidad desde el Convenio 108 del Consejo de Europa, de 28-1-1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981. Ratificado por España el 27 de enero de 1984.

No obstante, como ocurre con casi todos los comienzos, este primer enfoque fue criticado. Principalmente por impreciso y difícil de aplicar, pero también hubo críticas relativas a que no incidía lo suficiente en algunos principios como podía ser la minimización en la recogida de los datos. Sin embargo, no debemos dejar de resaltar que esta fue la primera vez que se introdujo la noción del mismo y que aquello dio pie a desarrollar y evolucionar un concepto que, a día de hoy, ya se encuentra recogido como un imperativo legal. [53]

Sin embargo, desde que Ann Cavoukian introdujo este enfoque hasta que ha sido recogido como imperativo legal, la privacidad desde el diseño ha pasado por múltiples

[52] ADDIN ELSHEKEIL, S., LAOYOOKHONG, S. *GDPR Privacy by Design From Legal Requirements to Technical Solutions* [en línea]. 2017. Disponible en: https://dsv.su.se/polopoly_fs/1.351720.1507815130!/menu/standard/file/Stipendie2017_ElShekeil-Laoyookhong.pdf

[53] GARCÍA HERRERO, J. *Privacidad desde el Diseño o "Privacy by Design" en el Reglamento General de Protección de Datos (I)* [en línea]. 08 de noviembre de 2016. Disponible en: https://jorgegarciaherrero.com/privacidad-desde-el-diseno-o-privacy-by-design-i/

fases y ha disfrutado de diferentes momentos de real protagonismo en determinadas sociedades.

Podemos entender que el primer reconocimiento internacional a este principio lo encontramos en octubre de 2010, concretamente en la Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, que tuvo lugar en Jerusalén. Aquí se confirmó que este principio es requisito imprescindible para la efectiva protección de la privacidad de toda persona física, dado que en aquel momento se entendía que la legislación, por sí sola, era insuficiente[54].

Otro claro ejemplo de la evolutiva importancia de este término es que en 2012 la Federal Trade Commision, dentro del contexto de la privacidad estadounidense, calificó la privacidad desde el diseño como un pilar fundamental para el marco normativo de la protección de datos americana.

La Doctora Cavoukian no se limitó a definir el término, sino que estableció siete principios que, a día de hoy, se conocen como fundamentales a la hora de diseñar nuevas tecnologías que permitan acceder y/o tratar datos de carácter personal.[55]

Ahora, con el RGPD, la protección de datos desde el diseño se ha convertido en un componente ya no solo esencial, sino obligatorio para toda compañía.

c. Principios

PRIMERO. - Proactivo, no Reactivo; Preventivo no Correctivo.

La idea principal de este enfoque es que ha de ser proactivo y debe poder anticiparse a cualquier evento que implique una invasión en la privacidad de los usuarios. La privacidad desde el diseño no debe aguardar a que los problemas se

[54] LEFEBVRE, F. *Memento Práctico Protección de Datos*. Editorial Jurídica Lefebvre®, 2019. ISBN 978-84-17544-49-2.

[55] CAVOUKIAN, A. *Privacy by Desing. The 7 Foundational Principles. Implmentation and Mappin of Fair Information Practices* [en línea]. Disponible en: https://www.iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf.

materializar y reaccionar a ellos corrigiéndolos, sino que debe prevenirlos y ofrecer medidas que puedan evitar que estos se produzcan.

SEGUNDO. - Privacidad como la Configuración Predeterminada.

La privacidad desde el diseño pretende que el usuario no tenga que realizar ninguna configuración concreta para proteger su privacidad, sino que los sistemas vengan preconfigurados de la forma más proteccionista posible. De esta manera, se garantiza el máximo grado posible de privacidad de forma automática y predeterminada.

TERCERO. - Privacidad Incrustada en el Diseño.

No se busca que la privacidad sea una capa extra o suplementaria, sino que venga incrustada en el diseño de la arquitectura de los sistemas y que sea una funcionalidad base más, que forme parte integral del mismo.

CUARTO. - Funcionalidad Total – "Todos ganan", no "si alguien gana, otro pierde".

Se pretende que no exista ninguna rivalidad entre privacidad y seguridad de tal modo que para garantizar la totalidad de una se deba renunciar a un poco de la otra[56]. La privacidad desde el diseño ha de buscar que todos los intereses legítimos de un usuario prevalezcan en igual medida sin necesidad de hacer ninguna concesión a cambio de nada.

QUINTO. - Seguridad Extremo-a-Extremo – Protección de ciclo de vida completo.

Es obvio que esta privacidad debe operar “extremo a extremo”, es decir, ha de formar parte de todo el flujo de los datos, en cada fase del ciclo de vida del sistema, esto es, desde el primer momento en el que se recogen los datos hasta que estos son destruidos al concluir la finalidad para la cual fueron recabados, incluyendo, obviamente, las garantías necesarias durante el tiempo que son retenidos.

[56] “¿Qué es el Privacy by Design?”. *Blog de protección de datos para empresas y autónomos – Grupo Ático 34.* 30 enero 2018. Disponible en: https://protecciondatos-lopd.com/empresas/privacy-by-design/

SEXTO. - Visibilidad y Transparencia.

La idea de la privacidad desde el diseño es ser capaz de demostrar que ha incluido satisfactoriamente todas las medidas necesarias. Para este, el sistema ha de ser verificable, para lo que ha de garantizar transparencia en cuanto a sus componentes y operaciones de tratamiento.

SÉPTIMO. - Respeto por la Privacidad de los Usuarios.

Esta es una máxima de este enfoque, pues ha de estar totalmente dirigido y centrado en asegurar la privacidad del usuario por encima de los posibles intereses de los responsables del tratamiento. Para ello, se han de ofrecer todas las facilidades posibles al usuario, como un sistema adecuado de notificaciones o una configuración fácilmente comprensible.[57]

2. Privacidad desde el diseño en la normativa actual

Como habíamos adelantado, aunque el concepto se remonte 30 años atrás en el tiempo y haya sido objeto de múltiples opiniones y controversias por parte de reguladores de todo el mundo, la privacidad desde el diseño no ha sido una obligación legal hasta su reciente incorporación a la legislación europea, formando ahora parte del RGPD.

En este sentido, el de 2 junio de 2016 la propia AEPD señaló que alguno de los aspectos introducidos por la nueva norma "*constituyen la formalización en una norma legal de prácticas ya muy extendidas en las empresas o que, en todo caso, formarían parte de una correcta puesta en marcha de un tratamiento de datos, como pueden ser la privacidad desde el diseño y por defecto*".

En línea con esto, es curioso comprobar como en enero de 2009, Ann Cavoukian adelantó que este concepto simbolizaba un marco de protección de la privacidad en el futuro que sería, por defecto, el modus operandi de las organizaciones. La frase literal

[57] PUYOL MONTERO, J. *La privacidad responsable o la privacidad por el diseño*. Junio 2017

fue que "*Privacy by Design advances the view that the future of privacy cannot be assured solely by compliance with legislation and regulatory frameworks; rather, privacy assurance must become an organization's default mode of operation* (CAVOUKIAN, 2009)[58]".

Concretamente, el texto del que venimos hablando y que en breves entraremos a estudiar con detalle lo podemos encontrar en el Considerando 78 y en el Artículo 25 del RGDP, que venimos a reproducir literalmente:

Considerando 78 RGPD[59]

"[…] A fin de poder demostrar la conformidad con el presente Reglamento, el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto. […] Al desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que están basados en el tratamiento de datos personales o que tratan datos personales para cumplir su función, ha de alentarse a los productores de los productos, servicios y aplicaciones a que tengan en cuenta el derecho a la protección de datos cuando desarrollan y diseñen estos productos, servicios y aplicaciones […]"

Artículo 25 Protección de datos desde el diseño y por defecto[60]

"1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de

[58] CAVOUKIAN, A. *Privacy by Design. Information & Privacy Commissioner of Ontario* [en línea] Enero de 2009. Disponible en: https://www.ipc.on.ca/wp-content/uploads/2013/09/pbd-primer.pdf
[59] Considerando 78 RGPD. Disponible en: https://www.boe.es/doue/2016/119/L00001-00088.pdf
[60] Artículo 25 "Protección de datos desde el diseño y por defecto" RGPD. Disponible en: https://www.boe.es/doue/2016/119/L00001-00088.pdf

datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.

2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.

3. Podrá utilizarse un mecanismo de certificación aprobado con arreglo al artículo 42 como elemento que acredite el cumplimiento de las obligaciones establecidas en los apartados 1 y 2 del presente artículo."

Lo que deja claro este precepto es que, a partir de la entrada en vigor del RGPD, la privacidad desde el diseño es un requisito más que todo RT ha de observar y tener en cuenta.

No obstante, el precepto es ambiguo y hace depender la aplicación del concepto de factores poco objetivos como son "el estado de la técnica", "el coste de la aplicación", la "naturaleza" o los "riesgos" del tratamiento. Por tanto, se estima necesario intentar realizar un humilde acercamiento a la posible intención que tenía el regulador cuando hizo depender la implementación de la PdD de estos preceptos.

a. Análisis del artículo 25.1 RGPD (Protección de datos desde el diseño)

De acuerdo con el artículo, los responsables del tratamiento deberán aplicar "*medidas técnicas y organizativas apropiadas*" así como integrar "*las garantías necesarias*" de cara a aplicar los principios de protección de datos del RGPD y proteger así los derechos de los interesados. Por tanto, podemos concluir que estas medidas y

garantías perseguirán un objetivo idéntico, a saber, la salvaguarda de los derechos de los interesados, garantizando una adecuada protección de sus datos de carácter personal. El RGPD no obliga a los responsables a aplicar medidas y garantías preestablecidas, sino que otorga libertad para analizar el tratamiento y llevar a cabo las actuaciones que cada uno considere convenientes. Esta es una muestra de la subjetividad que a continuación vamos a analizar.

De cualquier modo, el artículo en cuestión sí indica que estas medidas/garantías han de ser efectivas para aplicar los principios de protección de datos. Para demostrar el carácter efectivo de estas medidas, entendemos que el responsable habrá de ser capaz de demostrar (i) que ha aplicado estas medidas/garantías y (ii) que las mismas son las necesarias y han servido para garantizar los derechos y libertades de los interesados. Con esto queremos decir que no va a ser suficiente con que los sujetos obligados por este artículo apliquen correctamente lo que aquí se les exige, sino que han de ser capaces de documentar el efecto real que tienen.

No obstante lo anterior, es igualmente relevante que el propio artículo 25 determina todos los factores que un RT ha de observar antes de designar qué medidas ha de incluir para una operación concreta de tratamiento. Estos factores son:

- *"El estado de la técnica":* Entendemos que el legislador ha querido que el RT se mantenga al día en cuanto a novedades tecnológicas que le permitan garantizar la efectividad de sus medidas. Por tanto, el responsable habrá de estar atento al progreso tecnológico del mercado y mantener unos sistemas lo más actualizados posibles, sin dejar de observar el resto de los factores.[61]

- *"El coste de la aplicación"*: Cuando hablamos de coste no nos referimos exclusivamente al económico. También se han de observar los recursos

[61] EDPB PLENARY MEETING. *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Adopted on 13 November 2019* [en línea]. 13 de noviembre de 2019. Disponible en: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf

(materiales, humanos, temporales, etc.) de los que se dispone en relación con los que se estima que son necesarios para llevar a cabo la implantación de la privacidad desde el diseño, y el mantenimiento de las medidas para garantizar la protección del interesado durante todo el ciclo de vida del tratamiento. Es decir, el responsable debe saber cómo gestionar todos los costes para aplicar la privacidad desde el diseño, pero no puede obviarla, pues, como bien nos recuerda la European Data Protection Board en sus Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Adopted on 13 November 2019 "*La incapacidad para soportar los costes no es excusa para no cumplir con el RGPD*[62]"

- *"La naturaleza, ámbito, contexto y fines del tratamiento"*: Esto implica que el responsable habrá de observar las características concretas del tratamiento, el alcance y el objetivo del mismo, así como las expectativas de los interesados. Todo ello le permitirá conocer mejor la relevancia y el impacto de dicho tratamiento y actuar en consecuencia.

- *"Los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas"*: Muy en línea con los factores anteriores (*naturaleza, ámbito, contexto y fin)*, pues conocer los riesgos del tratamiento, medidos estos a través de la probabilidad de ocurrencia y la gravedad que conllevaría la misma, permiten al RT conocer la magnitud de las medidas que ha de implementar.

b. Análisis del artículo 25.2 RGPD (Protección de datos por defecto)

Como podemos comprobar, la privacidad desde el diseño comparte artículo con lo que conocemos como "privacidad por defecto". No siendo este un concepto en el que

[62] EDPB PLENARY MEETING. Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Adopted on 13 November 2019 [en línea]. 13 de noviembre de 2019. Disponible en: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf

ahora deseemos ahondar, sí consideramos oportuno entrar a hacer una presentación rápida del mismo.

Lo que en el segundo apartado del artículo 25 RGPD se pretende es exigir que cualquier RT, por defecto (valga la redundancia) sea suficiente consciente de que solo ha de tratar aquellos datos personales que sean estrictamente necesario para la finalidad que persiga con el tratamiento. Esto atañe tanto a la intención del responsable como, y sobre todo, a la configuración que el sistema que trate estos datos tenga predeterminada. Es decir, esta protección por defecto incide en las decisiones que un RT debe hacer a la hora de establecer los valores de configuración que vengan predeterminados en su sistema en cuanto a qué datos va a tratar, qué cantidad de los mismos, la duración del tratamiento, etc. [63]

Esto es así porque se entiende que, de no serlo, los interesados podrían verse abrumados por las múltiples opciones de configuración que un sistema incluye al no tener, previsiblemente, las capacidades técnicas suficientes para entender realmente las implicaciones que esta configuración pueda tener sobre su privacidad. Por tanto, son los responsables del tratamientos quienes deben decidir estas opciones en nombre del interesado, posicionándose, claro está, a favor de la protección de los datos personales de estos últimos.

c. Análisis del artículo 25.3 RGPD (mecanismo de certificación)

Este apartado merece, al menos, una fugaz mención, pues como veremos a continuación es compleja y etérea la demostración de si una empresa ha implementado, o no, esta privacidad desde el diseño, pero en este apartado del artículo 25 parece que el legislador traslada al lector su intención de, en un futuro, poder acreditar de alguna manera el cumplimiento del principio de protección de datos desde el diseño gracias a determinadas certificaciones.

[63] European Data Protection Supervisor. *Preliminary Opinion on Privacy by Design 5/2018* [en línea]. 31 de mayo de 2018. Disponible en: https://edps.europa.eu/sites/edp/files/publication/18-05-

Pues bien, el artículo 42 RGPD[64] establece que "*Los Estados miembros, las autoridades de control, el Comité y la Comisión promoverán, en particular a nivel de la Unión, la creación de mecanismos de certificación en materia de protección de datos y de sellos y marcas de protección de datos a fin de demostrar el cumplimiento de lo dispuesto en el presente Reglamento en las operaciones de tratamiento de los responsables y los encargados.*".

De esto podemos deducir que el legislador europeo se da cuenta de la complejidad que va a suponer demostrar si se está o no cumpliendo este principio, por lo que abre la puerta a una futura certificación que establezca ciertas mediciones claras y objetivas que permitan evaluar y acreditar el cumplimiento de las obligaciones que este enfoque exige.

d. Sujetos obligados

Analizando un poco el artículo que nos atañe, es importante conocer quiénes son los sujetos obligados a seguir este camino de la privacidad desde el diseño.

Podemos indicar que toda organización (privada o pública) que trate datos de carácter personal, siempre y cuando el propio RGPD sea de aplicación de acuerdo con los artículos 2 y 3, en los que se regulan los ámbitos de aplicación material y territorial, respectivamente, habrá de estar sujeto a la filosofía de la privacidad desde el diseño. Más concretamente, podemos advertir que este concepto está particularmente dirigido a los creadores y desarrolladores de los sistemas que tratan los datos, aunque es igualmente aplicable a toda empresa que lleve a cabo un tratamiento de datos personales, pues habrá de implementar dentro de su compañía las medidas necesarias para cumplir con este principio.

[64] Artículo 42 "Certificación" RGPD. Disponible en: https://www.boe.es/doue/2016/119/L00001-00088.pdf

No obstante, aunque esta obligación recaiga claramente sobre los RT, la misma ha de servir de utilidad para cualquier proveedor de tecnología que, aunque no venga expresamente mentado en el precepto 25 del RGPD[65], puede encontrar en estas directrices una orientación sobre cómo desarrollar sus productos de tal forma que esto suponga una ventaja competitiva, pues ayudará a los responsables del tratamiento a cumplir con sus obligaciones.

El incumplimiento de la obligación de implementar las medidas necesarias para cumplir adecuadamente con la protección de datos desde el diseño se considerará una infracción grave cuya sanción, que viene recogida en el artículo 83.4 RGPD[66], puede llegar a ser de hasta 10.000.000 EUR o de una suma igual al 2 % del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía[67].

[65] Artículo 25 "Protección de datos desde el diseño y por defecto" RGPD. Disponible en: https://www.boe.es/doue/2016/119/L00001-00088.pdf

[66] Artículo 83 "Condiciones generales para la imposición de multas administrativas" RGPD. Disponible en: https://www.boe.es/doue/2016/119/L00001-00088.pdf

[67] A título informativo, en la web https://www.enforcementtracker.com/# podemos encontrar una lista de las sanciones que las distintas autoridades de protección de datos de los Estados Miembros han impuesto en sus países en virtud del RGPD. Así, desde que el RGPD fuera de aplicación, y hasta la fecha, a nivel europeo se han producido las siguientes multas por incumplimiento del artículo 25 RGPD, ordenadas de más antiguas a más recientes:

- La primera tuvo lugar el 27 de junio de 2019, cuando la Autoridad Nacional Supervisora de Tratamiento de Datos Personales de Rumania impuso una multa de 130.000 € a UNICREDIT BANK SA por considerar que el banco no había aplicado medidas técnicas y organizativas adecuadas, lo que generó la fuga de identificadores y direcciones de hasta 337.042 titulares de interesados, entendiendo que esta insuficiencia de medidas contravenía los artículos 25.1 y 5.1.c RGPD.
- El segundo de los casos lo encontramos en Bulgaria, donde el 03 de septiembre de 2019, la Comisión de Protección de Datos Personales de este país impuso dos sanciones de 1.022 euros y 5.113 euros a un prestador de servicios de telecomunicaciones por llevar a cabo un tratamiento ilícito de datos personales de un interesado. En su resolución, la autoridad entendió que los artículos que se vieron afectados fueron el 6.1 y el 25.1 RGPD.
- El 07 de octubre de 2019, Autoridad Helénica de Protección de Datos impuso una multa de 200.000 euros a otro proveedor de servicios de telecomunicaciones debido a que varios de sus clientes fueron objeto de telemarketing a pesar de haber declarado expresamente su oposición para ello. Según entendió la autoridad griega, los errores técnicos llevaron a que estas oposiciones fueran ignoradas, errores que se debían a una mala aplicación del artículo 25.1 RGPD.
- La penúltima de las multas la encontramos en Alemania, cuando el 30 de octubre de 2019 la Autoridad de Protección de Datos de Berlín impuso a Deutsche Wohnen SE una multa por valor de 14.500.000 euros, debido a que esta empresa empleaba un sistema de almacenamiento de datos personales que no incluía la posibilidad de eliminar datos que ya no eran necesarios. De este modo, fue posible acceder a datos personales de interesados que habían sido almacenados durante muchos años sin que siguieran sirviendo para la finalidad para la que fueron recabados. Los artículos que se entendieron afectados fueron el artículo 5 y el 25 RGPD.
- Por último, recientemente el 10 de diciembre de 2019, y de nuevo la Autoridad Nacional Supervisora de Tratamiento de Datos Personales de Rumania, ha impuesto una multa de 14.000 euros a la empresa Hora Credit IFN SA debido a una denuncia en la que se alegaba que esta compañía transmitía

e. Razonamiento de los requisitos de privacidad desde el diseño

Antes de entrar a enumerar y analizar las distintas estrategias de las que se pueden valer los responsables del tratamiento para implementar correctamente la privacidad desde el diseño, debemos realizar un último inciso para terminar de entender el alcance del artículo 25 del RGPD.

Las últimas palabras del primer apartado del artículo 25 RGPD establecen que las medidas han de ser *"…concebidas para aplicar de forma efectiva los principios de protección de datos…".*[68]

Por tanto, el razonamiento que encontramos detrás de esta filosofía es la de aplicar los principios de protección de datos presentes en el RGPD, que servirán como base para determinar si los sistemas han logrado o no una adecuada protección de datos por diseño. Aunque estos principios han sido explicados anteriormente en el segundo apartado del cuarto punto del presente documento, nos limitaremos aquí exclusivamente a recordar que estaban recogidos en el artículo 5.1 RGPD y que eran: (i) licitud, lealtad y transparencia; (ii) limitación de la finalidad; (iii) minimización de datos; (iv) exactitud; (v) limitación del plazo de conservación; y (vi) integridad y confidencialidad.[69]

Igualmente, con anterioridad se ha explicado el segundo apartado del mismo artículo, que incorpora otra novedad interesante, el principio de responsabilidad proactiva, que recordemos que imponía al RT la responsabilidad de demostrar el cumplimiento de todo lo dispuesto en el primer apartado del mismo artículo 5 RGPD.

---

documentos con datos personales a direcciones de correo erróneas. La investigación que desencadenó esta denuncia determinó que la empresa trataba datos sin aplicar medidas eficaces para verificar la exactitud de los datos recopilados. La autoridad entendió que tampoco se habían tomado medidas de seguridad suficientes para evitar una divulgación no autorizada de datos personales de terceros, viendo así violados tanto el artículo 5 como el 25 RGPD.

[68] Artículo 25 "Protección de datos desde el diseño y por defecto" RGPD. Disponible en: https://www.boe.es/doue/2016/119/L00001-00088.pdf

[69] Artículo 5 "Principios relativos al tratamiento" – RGPD. Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807

3. Estrategias de diseño de la privacidad

Analizado todo lo anterior, es hora de preguntarnos cómo se concreta la privacidad desde el diseño lo suficiente como para que las empresas puedan aplicarla en la práctica.

Como hemos visto, esta filosofía busca que los desarrolladores inserten determinadas preconfiguraciones técnicas que mejoren la privacidad del sistema en su conjunto desde la fase de diseño de un producto. Por tanto, es importante conocer que el diseño de un producto es un proceso que cuenta con distintas fases, a saber: concepción, análisis, diseño, desarrollo, operación, mantenimiento y retirada. La AEPD, en su guía de privacidad desde el diseño, ilustra muy bien estas fases, a saber: (i) Concepción; (ii) Análisis; (iii) Diseño; (iv) Desarrollo; (v) Operación; (vi) Mantenimiento; y (vii) Retirada.

Es interesante observar como la AEPD opina que las estrategias de diseño de la privacidad han de ser introducidas entre las fases de concepción y análisis. Igualmente, recomienda que los patrones de diseño de la privacidad sean contemplados entre las fases de análisis y diseño y, por último, cree oportuno que las PETs (Privacy Enhancing Technologies) se tengan en consideración entre la fase de diseño y la de desarrollo.[70]

Podemos comprobar cómo se determinar que las estrategias que se deben llevar a cabo se han de tener en cuenta desde la primera fase del ciclo. En este momento, y de cara a garantizar el éxito del proceso de diseñar la privacidad, habrá que asegurarse de representar en el producto no solo los intereses del RT, sino también los intereses de privacidad de los interesados cuyos datos personales sean procesados.

[70] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Guía de Privacidad desde el Diseño* [en línea]. Disponible en: https://www.aepd.es/sites/default/files/2019-11/guia-privacidad-desde-diseno.pdf

En total podemos encontrar 8 estrategias de diseño de la privacidad diferentes, que las podemos dividir en dos grupos principales, a saber, las orientadas a datos y las orientadas a procesos.

Las 4 primeras (orientadas a datos) serían: (i) minimizar; (ii) abstraer; (iii) separar; y (iv) ocultar. Las otras 4 (orientadas a procesos) serían: (v) controlar; (vi) cumplir; (vii) demostrar; y (viii) informar.

Que haya 8 estrategias no significa que el responsable deba elegir una y concentrarse en implementarla, obviando el resto de las mismas[71]. Todas tienen su utilidad y cada una ayuda a cumplir con el objetivo de la privacidad desde el diseño, que no olvidemos que es la de garantizar que se cumplen los principios del RGPD. Por tanto, el seguimiento y aplicación de todas ellas ayudará en enorme medida a lograr un producto respetuoso y concienciado con la privacidad de los interesados. Por ello, procedemos a realizar un repaso por todas ellas.

a. Minimizar

Probablemente esta sea la estrategia más obvia de todas y consiste en minimizar los datos que se tratan. Como inteligentemente indica Jaap-Henk Hoepman en su documento Privacy Design Strategies (The Little Blue Book) de octubre de 2019 *"Nada puede salir mal con los datos que no se recopilan[72]"*.

Además, esta estrategia es abordable desde una doble perspectiva, pues la minimización de los datos puede darse tratando datos de menos interesados o tratando menos tipos de datos de los interesados.

Para llevar a cabo esta estrategia es importante determinar desde el inicio cuales son los interesados efectivamente relevantes y, de ellos, qué datos son realmente

[71] HOEPMAN, JH. *Privacy Design Strategies (The Little Blue Book)* [en línea]. 16 de octubre de 2019. Disponible en: https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf
[72] HOEPMAN, JH. *Privacy Design Strategies (The Little Blue Book)* [en línea]. 16 de octubre de 2019. Disponible en: https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf

necesarios. Cuando se tenga la respuesta, se habrán detectado los datos que son relevantes para el tratamiento y, a partir de ahí, la idea es tratar exclusivamente esos datos seleccionados. [73]

Las tácticas que se pueden seguir para llevar a cabo esta estrategia son (i) excluir todo aquello (interesados y datos) que no sea realmente necesario; (ii) eliminar parcialmente aquellos datos que dejen de ser necesarios; y (iii) suprimir definitivamente aquellos datos que dejen de ser relevantes para la finalidad para la que fueron recabados, asegurando que estos datos no pueden ser recuperados.

Como podemos observar, algunas de estas técnicas están íntimamente relacionadas con el principio de limitación del plazo de conservación, pues supone fijar de antemano un periodo de retención de los datos a partir de cual estos habrán de ser borrados.

b. Separar

La segunda de las estrategias consiste en separar los datos de tal forma que no sea posible, o al menos tratar de dificultar, la combinación o correlación de los datos que puedan pertenecer a un mismo interesado.

Para ello, se podrá recopilar o tratar los datos en diferentes bases de datos o incluso contar con distintos espacios físicos entre los que distribuir los datos. Un ejemplo que nos permitirá visualizar la estrategia de la separación es la táctica empleada por la empresa Apple, pues el sistemas operativo iOS10 crea carpetas de fotos en función de los interesados que aparecen en ellas utilizando tecnología de reconocimiento facial. El software que se utiliza para esto se ejecuta localmente en cada dispositivo móvil, sin que esta información sea compartida con otro dispositivo y sin que se envíe a ningún servidor central, por tanto Apple no llegar a tratar esta información. [74]

[73] GUTIÉRREZ LISARDO, J.I. *Los mediadores ante el reto de la adaptación al RGPD*. Febrero 2019
[74] HOEPMAN, JH. *Privacy Design Strategies (The Little Blue Book)* [en línea]. 16 de octubre de 2019. Disponible en: https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf

c. Abstraer

Esta estrategia consiste en limitar el detalle con el que se va a proceder al tratamiento de los datos. Aunque a priori pueda sonar un poco abstracta, las tácticas a seguir para lograrlo pasan por generalizar algunos de los datos que se tratan, usando atributos como puede ser la edad en vez de otros más específicos como podría ser la fecha de cumpleaños.

Similar al ejemplo anterior, podríamos considerar perturbar la información de tal manera que se añada una capa de información al dato real que se quiere tratar. Por ejemplo, en vez de tratar un valor exacto como podrían ser las coordinadas de un interesados, se reportará esta misma ubicación pero dentro de un rango de distancia superior.

Una gran herramienta cuyo uso está aumentando es la encriptación homomórfica[75], un tipo de cifrado de información que tiene la propiedad de permitir realizar ciertas operaciones sobre los datos cifrados sin necesidad de descifrarlos. Por ejemplo, podrías tener dos cantidades cifradas con este tipo de encriptación y podrías sumarlas sin descifrarlas y obtendría un resultado cifrado de dichas suma que al descifrarlo coincidiría con la suma realizada sobre las cantidades sin cifrar.

d. Ocultar

Esta sería la última de las estrategias basadas en datos y, como el propio nombre indica, consiste en proteger los datos de carácter personal de manera que sean confidenciales, es decir, que nadie pueda acceder a ellos y observarlos.

Para lograr llevar a cabo esta estrategia, se puede (i) proteger los datos restringiendo el acceso a la base de datos sólo a aquellas personas que sea estrictamente necesario y acompañar este gesto con una adecuada política de accesos;

[75] CAVOUKIAN, A. *Global privacy and security, by design: Turning the "privacy vs. security" paradigm on its head* [en línea]. 12 de julio de 2017 . Disponible en: https://link.springer.com/content/pdf/10.1007%2Fs12553-017-0207-1.pdf

(ii) disociándolos, esto es, sí se conocen los datos pero es imposible identificar a qué persona pertenecen; (iii) ofuscándolos, lo que impediría la comprensión de la misma a cualquier tercero que accediera sin permiso a estos datos; o (iv) haciéndolos inobservables del todo, lo que impediría que nadie fuera si quiera consciente de la existencia de los mismos.

Algunas herramientas de encriptación estándares pueden ser utilizadas para ocultar esta información como veremos más adelante.

e. Informar

Esta sería la primera de las 4 estrategias que están orientadas a los procesos de la compañía más que a los datos tratados en sí.

Esta es una estrategia fundamental, totalmente alineada con el principio de transparencia que recoge el artículo 5.1 RGPD, pues es imperativo que el interesado esté debidamente informado sobre los tratamientos que se realizan sobre sus datos personales: quien los está tratando, cómo lo está haciendo, para qué, etc. Además, esta información ha de ser trasladada con claridad, pues el fin de esta información es que el usuario esté en plenas condiciones para tomar decisiones informadas sobre cómo se está tratando su información personal y así decidir sobre su privacidad.

Esta información se suele transmitir al interesado en lo que se conoce como política de privacidad con carácter previo a la contratación por parte de un cliente de un producto que lleve asociado un tratamiento de sus datos de carácter personal. En estos momento, el RT habrá de comunicar al interesado su política de privacidad asociada a dicho tratamiento.

En este documento, el RT deberá tratar de trasladar al interesado que una de sus prioridades es la privacidad y la seguridad de los datos que va a tratar.

Esta política debe transmitir mensajes de transparencia con el interesado respecto a los datos que se van a recoger sobre este y explicándole por qué y para qué se utilizan, dando una especial garantía de que estos datos no se tratarán de una inesperada, oscura o abusiva.

Igualmente, esta política debe tener una clara visión de que el único que puede controlar el uso que se hace de los datos es el propio interesado, por lo que el RT debe poner a su disposición las herramientas necesarias para que pueda decidir en todo momento cómo quiere que sean tratados los datos, hasta cuándo y cómo puede acceder y actualizar su información personal.

Por último, como no puede ser de otra manera, el RT ha de preocuparse por garantizar la seguridad, el secreto y la confidencialidad de estos datos, por lo que debe transmitir que adopta las más exigentes y robustas medidas de seguridad para evitar pérdidas, alteraciones, malos usos o accesos sin autorización.

Al amparo de estos tres principios que deben transmitir la política de privacidad (transparencia, control y seguridad), las preguntas que el RT deberá responder al interesado serán:[76]

1. ¿Quién es RT? Aquí el responsable habrá de dar su denominación social completa, su CIF, dirección y, preferiblemente, una dirección de correo a la que escribir.

2. ¿Qué datos van a ser tratados? Indicando que los datos tratados son los estrictamente necesarios para prestar adecuadamente el servicio, será conveniente indicar la tipología de datos que se tratan (especiales, identificativos, características personales, detalles de empleo, circunstancias

[76] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Informe sobre políticas de Privacidad en internet. Adaptación al RGPD* [en línea]. Septiembre 2018. Disponible en: https://www.aepd.es/sites/default/files/2019-09/informe-politicas-de-privacidad-adaptacion-RGPD.pdf

sociales, transacciones de bienes y servicios, académico-profesionales, económico-financieros, información comercial y datos de tráfico)

3. ¿Cómo se obtienen estos datos (de dónde proceden)? Aquí se deberá detallar la forma de entrada de los datos, que bien puede ser porque el interesado complete determinados campos con información suya o, por ejemplo, que los datos se obtengan de fuentes de acceso público, que sean datos calculados, etc.

4. ¿Para qué se utilizan estos datos? Este punto es fundamental, pues habrá que explicar, de la forma más sencilla y a la vez más completa posible, la finalidad del tratamiento, es decir, dar al interesado una justificación de qué va a recibir a cambio del tratamiento que se hace de sus datos.

5. ¿Durante cuánto tiempo van a ser conservados? Como seguramente indique el resto de los términos y condiciones bajo los cuales se comercialice el producto, los datos serán almacenados el tiempo necesario para la prestación del servicio. No obstante, si por alguna razón estos datos van a ser conservados tras acabar este periodo, habrá que indicar ese periodo de tiempo y la razón por qué conservar los datos más tiempo del estrictamente necesario para la prestación del servicio.

6. ¿Quién tiene acceso a los mismos? En caso de que, además del Responsable, terceros tuvieran acceso a los datos personales del interesado, el responsable tendrá que indicarlo aquí, especificando que el acceso a estos datos que se proporciona a los terceros será siempre para finalidades lícitas y sólo durante el periodo de tiempo estrictamente necesario para ello.

7. ¿Cuáles son los derechos del interesado y cómo puede controlar sus datos? El RT debe indicar expresamente al interesado que podrá ejercer todos sus derechos en cualquier momento y de forma gratuita. Para ello, se deberá facilitar al interesado un canal para hacerlo. Lo ideal sería darle, entre otras, la opción de ejercerlos enviando un correo electrónico, aportando fotocopia de su DNI (o

documento equivalente) e identificando el derecho que solicita. Por último, habrá que indicar que el interesado tiene derecho a presentar una reclamación ante la autoridad nacional de control competente en materia de protección de datos.[77]

8. ¿Cómo protege el Responsable estos datos? Por último, en línea con uno de los principios integradores de la política de privacidad, habrá que indicar que el responsable garantiza la seguridad, el secreto y la confidencialidad de los datos y que, para ello, ha adoptado las medidas de seguridad oportunas.

Toda esta información situará al sujeto en una posición óptima para consentir o no, con conocimiento de causa, el tratamiento sobre sus datos personales.

Igualmente importante será la información que un responsable habrá de trasladar al usuario en cuanto sea consciente de que se ha producida una brecha de seguridad que ha implicado la fuga de los datos. Es conveniente que las empresas cuenten con procedimientos claros que indiquen como actuar en estos casos.

Es cierto que, con toda la información que se exige que se le traslade al interesado, a veces se le sobrecarga de texto y se logra, aun con toda la buena intención, un efecto contrario al inicialmente deseado. Es por ello que se está trabajando en maneras más sencillas de informar y notificar a los usuarios finales. A tal fin, y al igual que sucede con los iconos creados por Creative Commons para informar sobre los derechos de autor de un documento concreto, sería muy deseable contar en el futuro con pictogramas de privacidad que resumieran estas políticas de privacidad.

Un gran ejemplo de notificación no invasiva es el que usa la empresa Apple para notificar en los iPhones cuando el dato de la ubicación se está tratando, pues aparece una flecha en la barra superior del móvil, informando de forma muy sutil pero

[77] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Protección de Datos: Guía para el Ciudadano* [en línea]. Disponible en: https://www.aepd.es/sites/default/files/2019-10/guia-ciudadano.pdf

totalmente clara y transparente que el sistema ha accedido a los servicios de localización.

f. Controlar

El usuario, como propietario de los datos personales que van a ser tratados, debe tener el control sobre los mismos y sobre las actividades de tratamiento que sobre ellos se lleven a cabo. Por tanto, los productos deben estar diseñados de tal manera que permitan al usuario tener un control adecuado sobre el tratamiento de sus datos.

Para que esto se cumpla, una de las tácticas que se puede seguir sería pedir al usuario su consentimiento para que se produzca el tratamiento. El consentimiento es uno de los pilares del RGPD. En este sentido, el apartado 11 del artículo 4 RGPD define el consentimiento como "*Toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen*" [78]. Es decir, el propio RGPD especifica cómo habrá de ser el consentimiento que preste el usuario. Siendo así las cosas, el tipo de consentimiento que más se adecua a las exigencias del RGPD es el consentimiento explícito, quedando prohibidos los consentimientos tácitos mediante casillas marcadas por defecto. Igualmente, este consentimiento ha de ser retirable por el usuario, y esta retirada ha de ser tan fácil como lo fue otorgarlo. Por último, recae sobre el responsable la obligación de demostrar que dicho consentimiento ha sido obtenido siguiendo las instrucciones del RGPD.

Sin ánimo de entrar en detalle sobre lo siguiente, sólo resaltar que con el RGPD el consentimiento pasa a ser una base legitimadora más, por lo que aunque hayamos hecho una especial mención al mismo, no siempre va a ser necesario obtener el consentimiento del interesado, pues siguiendo el apartado f del artículo 6 RGPD, el tratamiento será igualmente lícito cuando este sea "*necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero,*

[78] Artículo 4 "Definiciones" – RGPD. Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807

siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales...".

g. Cumplir

Como demuestra este segundo grupo de estrategias, la privacidad desde el diseño no sólo se puede lograr mediante medios técnicos, también son necesarias medidas organizativas que ayuden a las compañías a cumplir con los principios del RGPD.

Esta estrategia es la más orientada a esta finalidad interna de las compañías, pues pretende garantizar que todo responsable cumpla con estos principios mediante políticas internas de actuación ante distintas eventualidades.

Para poder llevarla a cabo correctamente, la organización debe interiorizar la privacidad como un pilar más, creando una política de privacidad que contemple objetivamente sus fundamentos legales para llevar a cabo los tratamientos que realice y que sirva de carta de presentación ante sus clientes. Igualmente, debe contemplar en esta política las medidas técnicas y organizativas que efectivamente tiene implementadas, con roles y responsabilidades claramente asignados.

Por último, nunca se debe perder de vista que el tiempo y las circunstancias cambian, por lo que las políticas también han de hacerlo, comprometiéndose las organizaciones a actualizarlas regularmente en vez de considerar estas políticas como documentos estáticos.

h. Demostrar

Con esta estrategia los responsables del tratamiento darán respuesta al principio recogido en el apartado segundo del artículo 5 RGPD, es decir, al principio de responsabilidad proactiva, que como veníamos indicando anteriormente obliga a las

empresas a demostrar el cumplimiento de todo lo dispuesto en el apartado 1 del mismo precepto normativo.

Esta es una obligación nueva que ha traído consigo el RGPD, pero las tácticas que se pueden llevar a cabo son múltiples. Es recomendable que las empresas registren todas las decisiones, dejando por escrito las reuniones que han mantenido para tratar cualquier problema, los argumentos a favor y en contra de tomar una u otra decisión y, en general, crear un registro de todos los pasos que se han dado en el campo de la privacidad. Por otro lado, es conveniente llevar a cabo auditorías, bien internas bien externas, que permitan confirmar la efectividad de los procesos que la organización ha creado y compartir los resultados de dichas auditorias con la autoridad competente.

Una de las tácticas más recomendadas es la realización de evaluaciones de impacto de la protección de datos (PIA por sus siglas en inglés *Privacy Impact Assessment*). Normalmente, con un PIA limitado es suficiente y, cuando del mismo se derive que el tratamiento analizado puede suponer un alto riesgo para la privacidad de los interesados, se deberá realizar un PIA completo.[79]

Todo aquel que lleve a cabo un tratamiento de datos personales deberá tener documentados todos y cada uno de los tratamientos que realiza. Para ello, es recomendable que complete, para cada uno de los tratamientos que realiza, una adecuada ficha de actividad de tratamiento de datos personales.

Lo ideal sería que esta ficha recogiese, de cada tratamiento, la siguiente información:

- Datos del responsable: Denominación, dirección, datos de DPO si lo tiene, persona o equipo que dentro de la compañía es RT.

[79] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Guía práctica para las Evaluaciones de Impacto en la Protección de los datos sujetas al RGPD* [en línea]. Disponible en: https://www.aepd.es/media/guias/guia-evaluaciones-de-impacto-rgpd.pdf

- Datos del tratamiento: Descripción del servicio, la finalidad del tratamiento, tipología de datos personales, si hay o no ET y/o sub-encargados del tratamiento (si los hay, listarlos), el periodo de retención y borrado de los datos,

- Información sobre la entrada/recogida de los datos: Quienes son los interesados (categorías y ejemplos), el origen de los datos, la forma de entrada de estos, la base legitimadora, medios y/o mecanismos para el ejercicio de los derechos, identificar si el tratamiento consiste en la elaboración de perfiles, si se toman decisiones automatizadas o si se incorpora inteligencia artificial a la misma.

- Información de la salida de los datos: Indicar si hay transferencias internacionales y/o cesiones.

Este ejercicio puede servir igualmente para cumplir con la obligación del artículo 30 RGPD sobre el registro de las actividades de tratamiento.

4. Patrones de diseño de la privacidad

Una vez tenemos claros cuales son los objetivos de la privacidad desde el diseño y la empresa ha definido las estrategias que quiere implementar en sus productos, es necesario empezar con el desarrollo.

Durante este trabajo, es altamente improbable no encontrar algún problema que habrá que solucionar. Y a la vez es altamente probable que este problema no sea la primera vez que le surge a un desarrollador, por lo que alguien antes se habrá enfrentado a él y, seguramente, lo habrá resuelto. Aquí es donde entran en juego los conocidos patrones de diseño de la privacidad, que no son otra cosa que soluciones a problemas que surgieron en el pasado (que alguien resolvió usando este patrón) y que ahora se pueden reutilizar. Por tanto, como dice Antonio Leiva *"Si la forma de solucionar*

ese problema se puede extraer, explicar y reutilizar en múltiples ámbitos, entonces nos encontramos ante un patrón de diseño de software."[80]

No queremos entrar a profundizar en este concepto, pues entendemos que pertenece más a un ámbito particularmente técnico de la privacidad del diseño que al teórico, que es en el que aquí queremos centrarnos, pero sí nos gustaría resaltar que algunos de los múltiples beneficios que tiene el empleo de estas soluciones son el ahorro de tiempo y la garantía de que estas soluciones funcionan. Por ello, aunque ninguna normativa obliga al empleo de estos patrones, es altamente recomendable su uso.

Un último comentario para evitar confusiones. Un mismo patrón de diseño podría ayudar a implementar más de una estrategia, por lo que no debemos pensar en cada patrón como solución exclusiva y cerrada a un solo inconveniente. Por tanto, es conveniente conocer los diferentes tipos de patrones, tener claras las estrategias que queremos implementar en el producto y, a partir de ahí, decidir el patrón más conveniente al tratamiento de datos que se vaya a llevar a cabo.

Si este apartado suscita mayor interés al lector, indicar que hay múltiples catálogos de patrones de diseño de la privacidad. En la Guía de Privacidad desde el Diseño de la AEPD se listan varios y es al anexo 1 de esta misma guía al que queremos hacer referencia, pues aquí la AEPD ha recogido su propia selección de 54 patrones de diseño[81].

5. Privacy Enhancing Technologies (PETs)

Finalmente, una vez han sido analizadas las estrategias y se ha decidido cual implementar, así como diseñados los patrones de privacidad más oportunos para el

[80] Patrones de diseño de software por Antonio Leiva | Software Craftmanship. Disponible en: https://devexperto.com/patrones-de-diseno-software/

[81] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Guía de Privacidad desde el Diseño* [en línea]. Disponible en: https://www.aepd.es/sites/default/files/2019-11/guia-privacidad-desde-diseno.pdf

producto en cuestión, quedaría la última fase, la implementación de estos conceptos en la fase de desarrollo del producto.

Para llevar a cabo esta implementación, es conveniente hacer uso de las múltiples soluciones TIC (*Tecnologías de la Información y la Comunicación*) que podemos encontrar en el mercado. No obstante, hay un tipo concreto de soluciones TIC que minimizan los riesgos de sufrir violaciones de privacidad. Estas soluciones concretas reciben el nombre de Privacy Enhancing Technologies (en adelante, "PETs").

Las PETs no dejan de ser un tipo de tecnología que permiten incorporar, en la fase de desarrollo de un producto, funcionalidades para minimizar o, directamente, suprimir, los posibles riesgos de incumplimiento de las reglas de privacidad.[82]

Es más, el concepto de privacidad desde el diseño nace a partir de estas PETs, a raíz de un informe que en 1995 realizaron de forma conjunta Ann Cavoukian y John Borking, lo que nos permite entender la interconexión que existe entre ambos. Realmente este informe se centró en la manera de anonimizar determinadas transacciones, pero autores, como Peter Hustinx reconocieron el papel que habían hecho Ann Cavoukian y John Borking en su trabajo en cuanto al diseño y funcionamiento de las PETs.[83]

Como venimos viendo a lo largo del presente documento, múltiples han sido los intentos de profundizar en la necesidad de que desarrolladores de tecnología y responsables del tratamiento interioricen el concepto de la privacidad desde el diseño, con mayor o menos éxito. Lo que sí podemos confirmar es que el hecho de que ahora esta filosofía sea un requisito legal del RGPD es una muestra de que el legislador europeo ha querido fomentar el uso de las PETs.

---

[82] SÁNCHEZ BARROSO, M. Á. *Privacidad por diseño y análisis de impacto en la privacidad: conceptos en la nueva regulación de protección de datos* [en línea]. 16 de abril de 2014. Disponible en: https://technologyincontrol2.wordpress.com/2014/04/16/privacidad-por-diseno/.

[83] "Privacy by design". *Wikipedia, the free encyclopedia*. 1 de enero de 2020. Disponible en: https://en.wikipedia.org/wiki/Privacy_by_design

Como ya hemos visto en el apartado de las estrategias, la privacidad desde el diseño tiene dos enfoques, por un lado, las estrategias orientadas a datos que se centraban en aquellos elementos que permiten una adecuada gestión de los datos a lo largo del ciclo de vida del propio producto; y, por otro, aquellas estrategias más enfocadas a procesos de la propia compañía que buscaban orientar las prácticas de las empresas hacia la protección de la privacidad de sus clientes. En este sentido, las PETs tienen la misma categorización, pues algunas de estas herramientas buscan la protección de la privacidad de los interesados mediante aplicaciones de cifrado o amonificación, mientras que hay otra categoría de PETs más destinadas a gestionar las obligaciones de la compañía para con la privacidad, como puede ser el caso de herramientas más administrativas.

No obstante lo anterior, otra categoría en las que podemos dividir las PETs, son PETS sustitutivas y PETs complementarias [84]

Las primeras, se centran en proteger la identidad del interesado, normalmente reduciendo la cantidad de información que se recoge del usuario o anonimizando la información recogida. Estas tecnologías no suelen ir incluidas en la propia arquitectura de los productos, sino que más bien son herramientas que emplean los usuarios finales para lograr esta finalidad.

En segundo lugar, las PETs complementarias, no se oponen a la recopilación y el uso de los datos, pero siempre y cuando estas acciones estén alineadas con las normas de privacidad y todos los requisitos legales. Es decir, estas herramientas están pensadas para asegurar que la recogida y el tratamiento de los datos cumplen con los principios legales de protección de datos. A diferencia de las anteriores, en este caso las empresas sí suelen implementar estos mecanismos en sus productos, con lo que logran una mejor imagen de estos de cara a sus clientes, pues demuestra que sus productos tienen un compromiso fuerte con la privacidad del usuario.

[84] RUBINSTEIN, I. *Regulating Privacy by Design* [en línea]. 2011. Disponible en: https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1917&context=btlj

Como vemos, no todas las PETs están destinadas a la anonimización, pero sí es cierto que actualmente estas son las más útiles, pues cualquier sistema que permita anonimizar una información logra que los requisitos legales aplicados a los datos de carácter personal pasen a un segundo plano, puesto que si la anonimización realmente impide identificar a un interesado, ese dato perdería el carácter de personal y, por tanto, dejarían de serle aplicables las normativas de protección de datos.

VI. CONCLUSIONES

La tecnología ha traído una visible comodidad a nuestras vidas, pero también nuevas amenazas a nuestra privacidad que no son tan fáciles de detectar. En este escenario es donde ha entrado en juego la ciberseguridad, un área de la informática que pretende facilitar productos y soluciones a empresas e individuos que garanticen la confidencialidad y el control sobre los datos de carácter personal.

En este contexto, la privacidad se ha convertido en uno de los pilares básicos sobre los que se construye la economía actual. Ha dejado de ser el "extra" que venía siendo hace unos años y se ha configurado como un derecho fundamental de los individuos, y como tal ha de ser protegido.

El legislador así lo ha entendido y se ha visto obligado a generar alrededor de la privacidad un entorno de confianza internacional sin el cual ningún país va a poder sustentar sus modelos de negocio en el largo plazo. De este modo, en el ámbito europeo, ha nacido el RGPD, una norma de enorme calado en el día a día de todos los Estados Miembros y de todas las compañías que en ellos operan. En España, este reglamento ha sido incorporado al derecho español por la LOPDGDD.

Juntos, RGPD y LOPDGG, rigen el día a día de aquellas compañías que acceden y/o tratan datos de carácter personal. Estas empresas, en aras de tratar los datos personales de los ciudadanos con la mayor legalidad, seguridad y transparencia posible, han de cumplir con una serie de principios básicos que vienen regulados en estas normas. Uno de estos principios, que por su novedad ha supuesto uno de los grandes

cambios que el RGPD ha traído consigo, es el principio de responsabilidad proactiva, o accountability, que implica la adopción de ciertas medidas que permitan cumplir (así como demostrar dicho cumplimiento) lo estipulado en el RGPD. Una de estas medidas, tal vez una de las más importantes, es la que tiene que ver con la aplicación de la protección de datos desde el diseño.

Hasta ahora, las indicaciones sobre cómo diseñar un sistema cuidadoso con la privacidad de los usuarios han sido muy abstractas, además de no ser esto una imposición legislativa. No obstante, con la entrada en vigor del RGPD, la implementación de la filosofía de privacidad por diseño ya se ha vuelto una obligación. Obligación que, tal y como hemos visto, puede acarrear importantes sanciones para quienes la incumplan.

A pesar de lo anterior, la privacidad desde el diseño sigue siendo un concepto confuso. En términos prácticos, implica la adopción de medidas (procedimientos, sistemas, políticas, etc.) que garanticen la seguridad de los datos personales desde antes incluso de empezar a tratarlos, evitando así poner en riesgo la privacidad de los interesados. Es decir, tiene un claro componente preventivo en vez de correctivo, que implicaría adoptar medidas cuando esta privacidad ya ha sido violada, que es justo lo que se pretende prevenir. No debemos olvidar que el objetivo principal de esta filosofía es permitir que, tanto RT como ET, cumplan con los principios que establece el RGPD y aseguren los derechos que poseen los interesados.

Sorprende sobremanera que algo tan obvio haya tardado tanto en llegar a ser una obligación. No obstante, se venía demostrando que la privacidad no estaba asegurada simplemente por el cumplimiento de las leyes que había hasta ahora, de modo que se ha tenido que obligar a las empresas a “imprimir” la privacidad en el alma de sus tecnologías y organizaciones.

Pero parece evidente que el legislador, al pretender que sea cada empresa la que adopte las medidas que cada una considere convenientes de acuerdo a los riesgos que haya detectado, ha creado un pequeño limbo en el que las organizaciones, al no contar

con un catálogo concreto de medidas, aún tienen serias dudas sobre cómo aterrizar en sus productos esta filosofía.

Por tanto, y con esto ya concluimos, a pesar de la actual ausencia de guías internacionales que orienten a las empresas en el proceso de implementación de medidas efectivas durante el diseño de sus productos, entendemos como un avance enormemente beneficioso para la sociedad en general, y para cada ciudadano en particular, que el RGPD haya creado una obligación legal como es el principio de la protección de datos desde el diseño. Esta inclusión no hace más que reforzar la creciente tradición de crear un entorno favorable en el que los ciudadanos sean realmente dueños de su información.

VII. BIBLIOGRAFÍA

ADDIN ELSHEKEIL, S., LAOYOOKHONG, S. *GDPR Privacy by Design From Legal Requirements to Technical Solutions* [en línea]. 2017. Disponible en: https://dsv.su.se/polopoly_fs/1.351720.1507815130!/menu/standard/file/Stipendie2017_ElShekeil-Laoyookhong.pdf

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *El Reglamento de Protección de Datos en 12 preguntas* [en línea]. Disponible en: https://www.lopdat.es/noticias/el-reglamento-de-proteccion-de-datos-en-12-preguntas

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Guía de Privacidad desde el Diseño* [en línea]. Disponible en: https://www.aepd.es/sites/default/files/2019-11/guia-privacidad-desde-diseno.pdf

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Guía del Reglamento General de Protección de Datos para responsables de tratamiento* [en línea]. Disponible en: https://www.aepd.es/sites/default/files/2019-09/guia-rgpd-para-responsables-de-tratamiento.pdf

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Guía práctica para las Evaluaciones de Impacto en la Protección de los datos sujetas al RGPD* [en línea]. Disponible en: https://www.aepd.es/media/guias/guia-evaluaciones-de-impacto-rgpd.pdf

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Informe sobre políticas de Privacidad en internet. Adaptación al RGPD* [en línea]. Septiembre 2018. Disponible en: https://www.aepd.es/sites/default/files/2019-09/informe-politicas-de-privacidad-adaptacion-RGPD.pdf

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. *Protección de Datos: Guía para el Ciudadano* [en línea]. Disponible en: https://www.aepd.es/sites/default/files/2019-10/guia-ciudadano.pdf

ALIÑO SEHWERERT, J.J. *Cómo implementar el Reglamento General de Protección de Datos en la empresa.* Abril 2018.

CAVOUKIAN, A. *Global privacy and security, by design: Turning the "privacy vs. security" paradigm on its head* [en línea]. 12 de julio de 2017. Disponible en: https://link.springer.com/content/pdf/10.1007%2Fs12553-017-0207-1.pdf

CAVOUKIAN, A. *Privacy by Design. Information & Privacy Commissioner of Ontario* [en línea] Enero de 2009. Disponible en: https://www.ipc.on.ca/wp-content/uploads/2013/09/pbd-primer.pdf

CAVOUKIAN, A. *Privacy by Desing. The 7 Foundational Principles. Implmentation and Mappin of Fair Information Practices* [en línea]. Disponible en: https://www.iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf.

CHINEA LÓPEZ, J. *La privacidad desde el diseño. ¿Por legalidad o responsabilidad? [en línea]*. 26 de diciembre de 2012. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/privacidad-desde-diseno

Complylaw Privacidad | Privacidad desde el diseño: Enfoque práctico y medidas a adoptar. Wolters Kluwer España. 20 de septiembre de 2019. Youtube. Disponible en: https://www.youtube.com/watch?v=yU7OgqIeY2w

Constitución Española. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1978-31229

COUNCIL OF THE EUROPEAN UNION. *Proposal for a 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). 27 de enero de 2012. Disponible en: http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%205853%202012%20INIT

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 respeta al tratamiento de datos personales y a la libre circulación de estos datos. Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-1995-81678

Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo. Disponible en: https://www.boe.es/doue/2016/119/L00089-00131.pdf

Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. Disponible en: https://www.boe.es/doue/2016/194/L00001-00030.pdf

EDPB PLENARY MEETING. *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Adopted on 13 November 2019* [en línea]. 13 de noviembre de 2019. Disponible en: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf

European Data Protection Supervisor. *Preliminary Opinion on Privacy by Design 5/2018* [en línea]. *31 de mayo de* 2018. Disponible en: https://edps.europa.eu/sites/edp/files/publication/18-05-

FUERTES NIETO, M. Informe sobre la vulneración de los derechos al Honor, Imagen y privacidad en el ámbito médico por uso de tecnología. Tutor: Fernando Fonseca Ferrandis. Universidad Carlos III de Madrid, Departamento de Derecho, Madrid, 2019.

GARCÍA HERRERO, J. *Privacidad desde el Diseño o "Privacy by Design" en el Reglamento General de Protección de Datos (I)* [en línea]. 08 de noviembre de 2016. Disponible en: https://jorgegarciaherrero.com/privacidad-desde-el-diseno-o-privacy-by-design-i/

GUTIÉRREZ LISARDO, J.I. *Los mediadores ante el reto de la adaptación al RGPD.* Febrero 2019.

HOEPMAN, JH. *Privacy Design Strategies (The Little Blue Book)* [en línea]. 16 de octubre de 2019. Disponible en: https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf

INSTITUTO NACIONAL DE ADMINISTRACIÓN PÚBLICA. MINISTERIO DE HACIENCIA Y ADMINISTRACIONES PÚBLICAS. *El Reglamento General de Protección de Datos. Módulo 1: Marco general para el tratamiento de datos personales* [en línea]. Disponible en: https://www3.gobiernodecanarias.org/cpji/gestionconocimiento/_recursos/proteccion_datos/resources/Modulo_1.pdf

Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-1982-11196

Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-1992-24189

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-1999-23750

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673&p=20181206&tn=2

LEFEBVRE, F. *Memento Práctico Protección de Datos*. Editorial Jurídica Lefebvre®, 2019. ISBN 978-84-17544-49-2.

"Privacy by design". *Wikipedia, the free encyclopedia*. 1 de enero de 2020. Disponible en: https://en.wikipedia.org/wiki/Privacy_by_design

Propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas). Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52017PC0010

PUYOL MONTERO, J. *La privacidad responsable o la privacidad por el diseño.* Junio 2017.

PUYOL MONTERO, J. *Pautas para la implantación del RGPD: Las relaciones entre el responsable y el encargado del tratamiento. El tratamiento de datos por terceros. Los contratos de prestación de servicios y las nuevas exigencias de la contratación*. Mayo 2018.

"¿Qué es el Privacy by Design*?". Blog de protección de datos para empresas y autónomos – Grupo Ático 34*. 30 enero 2018. Disponible en: https://protecciondatos-lopd.com/empresas/privacy-by-design/

Real Decreto-ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-2018-10751

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). Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807

RUBINSTEIN, I. *Regulating Privacy by Design* [en línea]. 2011. Disponible en: https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1917&context=btlj

SÁNCHEZ BARROSO, M. Á. *Privacidad por diseño y análisis de impacto en la privacidad: conceptos en la nueva regulación de protección de datos* [en línea]. 16 de abril de 2014. Disponible en: https://technologyincontrol2.wordpress.com/2014/04/16/privacidad-por-diseno/.

SEMPERE, FJ. *Crossover entre el RGPD y la nueva LOPD* [en línea]. 13 de diciembre de 2018. Disponible en: http://www.privacidadlogica.es/crossover-entre-el-rgpd-y-la-nueva-lopd/

"Statement by Vice-President Ansip and Commissioner Jourová ahead of the entry into application of the General Data Protection Regulation". *European Commission oficial website*. 24 de mayo de 2018. Disponible en: https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_18_3889

Sentencia de 20 de julio de 1993, STC 254/1993, ECLI:ES:TC:1993:254. Disponible en: http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/2383#complete_resolucion&completa

Sentencia de 30 de noviembre de 2000, STC 290/2000, ECLI:ES:TC:2000:290. Disponible en: http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/4274#extractos

Tratado de la Unión Europea y del Tratado de Funcionamiento de la Unión Europea. Versiones consolidadas. Protocolos. Anexos. Declaraciones anejas al Acta Final de la Conferencia intergubernamental que ha adoptado el Tratado de Lisboa. Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-Z-2010-70002

VEALE, M., BINNS, R., AUSLOOS, J. "When data protection by design and data subject rights clash". *International Data Privacy Law*. 2018. Vol. 8. No. 2. [consulta: diciembre de 2018]. doi:10.1093/idpl/ipy002. Disponible en: https://academic.oup.com/idpl/article-pdf/8/2/105/25113376/ipy002.pdf