FACULTAD DE DERECHO

La Regulación Ética y Moral de la Protección de Datos generada por el *Big Data*

Autor: Georg Boyan Grudow Alonso

5, E3 y B

Área de Filosofía del Derecho

Tutor: María Ángeles Bengoechea Gil

Madrid

Abril 2021

RESUMEN: El avance de las tecnologías informáticas en los últimos 20 años ha dejado un mundo interconectado y donde los datos han pasado a ser los protagonistas. La protección de datos ha aparecido con el fin de proteger los derechos fundamentales como el de la privacidad de los usuarios de las tecnologías, y por ende su relevancia es cada vez mas importante. Por ello, se analiza como la protección de datos es el reflejo de los derechos privados en el mundo online. Tras esto, se revisa la regulación de la protección de datos actual, y sus aportaciones en cuanto a mecanismos de control y derechos. Además, se trata también el futuro de la regulación del *Big Data* y las carencias actuales de esta. Día a día se evidencian nuevas incertidumbres, y ello conllevará a mejorar la regulación al respecto.

ABSTRACT: The evolution of information technologies in the last 20 years has left an interconnected world where data has become the protagonist. Data protection has appeared in order to protect fundamental rights such as the right to privacy of technology users, and therefore its relevance is getting more important every day. Hence, it is analyzed how data protection is the reflection of private rights in the online world. Following this, the current data protection regulation is reviewed, and its contributions in terms of control mechanisms and rights. Furthermore, the future of Big Data regulation and its current shortcomings are also discussed. Every day new uncertainties become evident, and this will lead to improve the regulation in this regard.

Palabras Clave:
Consentimiento, Privacidad, Mecanismos de Control, Regulación Ética.

Keywords:
Consent, Privacy, Control Mechanisms, Ethical Regulation.

ÍNDICE

Índice figuras

Índice tablas

Abreviaturas

CCPA*: California Consumer Privacy Act*

CE: Constitución Española

CEPD: Comité Europeo de Protección de Datos

IA: Inteligencia artificial

LOPD: Ley Orgánica de Protección de Datos Personales

LPODPGDD: Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales

RGPD: Reglamento General de Protección de Datos

SPAM: *Spamming*

TFUE: Tratado Fundamental de la Unión Europea

UE: Unión Europea

1 INTRODUCCIÓN

A lo largo de la historia, principalmente a mediados del siglo XXI, la evolución tecnológica ha brindado grandes avances a la sociedad. Este avance ha llegado a un punto donde la sociedad se encuentra totalmente digitalizada. Un mundo, en el cual, absolutamente todos y cada uno de nosotros como individuos dejamos tenemos un "sello digital" y una traza digital. Esta marca individual se conoce coloquialmente como "huella digital". Pero ¿qué ocurre con todas esas huellas? ¿Están protegidas? ¿Sabemos que uso hacen las empresas con ellas, y donde están almacenadas?

Mediante sus órganos jurídicos la sociedad busco en un primer momento proteger los derechos de cada individuo mediante la ley, es decir una ley realizada por los distintos órganos jurisdiccionales de cada país y que ha transcendido hasta órganos supra nacionales como la Unión Europea. A pesar de ello, y de dichas regulaciones sigue sin ser suficiente la ley y hay que plantear un debate ético, filosófico y moral.

Principalmente, hay que introducir el derecho de privacidad como el derecho en el cual se basa la protección de datos. Cuando se navega por la web, las búsquedas, las preferencias, las recomendaciones o los intereses quedan registrados en el propio motor de búsqueda que se utiliza. Se genera un nuevo aspecto del derecho de privacidad, que ha transcendido de lo conocido a incluso una faceta económica. Este aspecto ha crecido de manera que ya es posible conocer las tendencias en masa, las preferencias de personales y de la mayoría de sociedad. También segmentar la población y dar así una gestión y un servicio mucho más eficiente, dando lugar así a unos datos muy valiosos para las empresas.

Lógicamente tiene no se trata de algo perjudicial en un primer momento, sino que parece beneficioso para la sociedad, tanto para los ciudadanos, las empresas y los gobiernos. Pero, cuando se analiza, puede ser de una espada de doble filo, ya que tanto los datos como el tratamiento que se hace de ellos pueden influir en el propio comportamiento humano y en la libertad individual. Un claro ejemplo es la publicidad que se muestra al navegar en una simple web. Los anuncios están específicamente diseñados para que se presenten en cada individuo de manera que tenga un interés especifico en dicho producto. Algo que a simple vista no parece perjudicial ¿Por qué iba a molestar que enseñen

publicidad que interesa a la persona que hace una búsqueda? Pero, además puede haber otras connotaciones como es el caso del proyecto de Cambridge Analíticas en la modificación de aquellos votantes indecisos a la hora de votar el "Brexit". De manera que eran bombeados con publicidad a favor de la salida de Inglaterra de la Unión Europea, y así concienciados de forma inconsciente que voten a favor.

En la Unión Europea, el derecho de protección de datos, que engloba el derecho de privacidad, es tratado como un derecho fundamental de manera que está reconocido en Tratados de la Unión Europea, en la Carta de los Derechos Fundamentales de la Unión Europea, e incluso de forma más específica en el RGPD. Esta regulación busca principalmente "*la creación de perfiles y lo define como el análisis o la predicción de aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos y establece que las personas tendrán derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado que produzca efectos jurídicos sobre él o le afecte significativamente de modo similar."*[1]

El fin de esta regulación es básicamente que cuando se traten los datos como perfiles elaborados y produzcan efectos jurídicos, se deberá cumplir unas garantías.

A nivel ético se plantea un problema al existir una interacción tan drástica entre humanos y máquinas de manera que en vez de ser los humanos que influencian las máquinas sean estas las que influencian a los humanos. Se crea por ello tres aspectos que deben de establecerse e irrumpir en este problema:

1. **El tratamiento ético** de los datos, es decir hasta que punto hay que llegar para que la influencia y el manejo que se hace de estos mismos dejen de perjudicar a los individuos de manera que sus intenciones o/y preferencias se vean influenciadas de manera perjudicial, atentando así contra su principio de autonomía y de privacidad.

[1] Ortiz, P. (2018, 24 diciembre). La protección de datos, un asunto profundamente humano". Universidad Europea (Disponible en: https://www.elcomercio.es/sociedad/proteccion-datos-asunto-20181224165559-nt.html?ref=https:%2F%2Fwww.google.com; última consulta 01/04/2021)

2. **La transparencia:** todos los individuos tienen el derecho a acceder a sus datos y saber el uso se les están dando.
3. **Capacidad de elección:** hace referencia a la capacidad de decisión por parte de los individuos a elegir que hacer con sus datos.

Este trabajo trata de estudiar la regularización, los mecanismos de control y los derechos relevantes respecto a la protección de datos en el *Big Data*. Como objetivos secundarios se plantea describir el *Big Data*, revisar la regularización o legislación, estudiar los mecanismos de gobierno de control, y discutir los principios éticos y morales asociados a los derechos que se plantea en la regularización.

Con respecto a la metodología se parte de una aproximación teórica con un enfoque jurídico del derecho existente en la actualidad y la descripción del impacto que se presenta ante el avance rápido de la tecnología. Se analiza la legislación existente y los factores que influyen en regulación ética y moral de la protección de datos

2 EL BIG DATA Y EL INTERNET DE LA COSAS

A lo largo de las últimas décadas, con el desarrollo de internet de las cosas (en inglés, *Internet of things*) y las nuevas tecnologías, se ha evolucionado desde un mundo totalmente desconectado, a un punto en el cual todo está interconectado mediante los objetos cotidianos como de los teléfonos móviles, los coches, las casas, etc. Se generan una gran cantidad de datos que ocasionan un rastro personal en internet. Con el uso de las nuevas tecnologías el usuario deja información como las preferencias, las tendencias, cuáles son sus apetencias, qué compra, cuál es el deporte que practica, etc.

"Cuando se habla de *Big Data* se refiere a conjuntos de datos o combinaciones de conjuntos de datos cuyo tamaño (volumen), complejidad (variabilidad) y velocidad de crecimiento (velocidad) dificultan su captura, gestión, procesamiento o análisis mediante tecnologías y herramientas convencionales, tales como bases de datos relacionales y estadísticas convencionales o paquetes de visualización, dentro del tiempo necesario para que sean útiles."[2]

Este concepto o aspecto de los datos resulta de gran valía para las empresas ya que supone un gran avance en cuanto a los estudios de mercados y análisis de datos. Se trata de un gran progreso ya que permite, un avance en el sentido de la información, ya que esto permite a las empresas tratar datos masivos. Es decir, no le hace falta una encuesta de pocos usuarios si no datos a gran escala.

[2] Big Data: ¿En qué consiste? Su importancia, desafíos y gobernabilidad. (Disponible en: https://www.powerdata.es/big-data; última consulta 12/03/2021)

Los tipos de fuentes y de tipos de datos Se representan en la tabla 1.

Característica	
Fuentes de datos	Internet y móviles Internet de las Cosas. Sectoriales recopilados por empresas especializadas. Experimentales.
Tipos de datos	No estructurados: documentos, vídeos, audios, etc. Semi-estructurados: software, hojas de cálculo, informes. Estructurados: aquellos que se encuentran ordenados: tabla Excel, Hojas de cálculo, Bases de datos de cualquier otro tipo, Aplicaciones para realizar cuestionarios tipo test, Fichas estandarizadas de clientes, Encuestas a usuarios de un servicio.

Tabla 1: Big Data, tipos de datos y sus fuentes

Fuente: Big Data: ¿En qué consiste? Su importancia, desafíos y gobernabilidad, Disponible en: https://www.powerdata.es/big-data, Consultado 12 de febrero de 2021

El Big Data presenta cinco grandes características llamadas las 5V que son: volumen (*volumen*), variedad (*variety*), velocidad (*velocity*), veracidad o validez (*veracity or validity*) y valor (*value*).[3] (Figura 1)

[3] Marr, B. (2016). *Big data in practice: how 45 successful companies used big data analytics to deliver extraordinary results*. John Wiley & Sons.

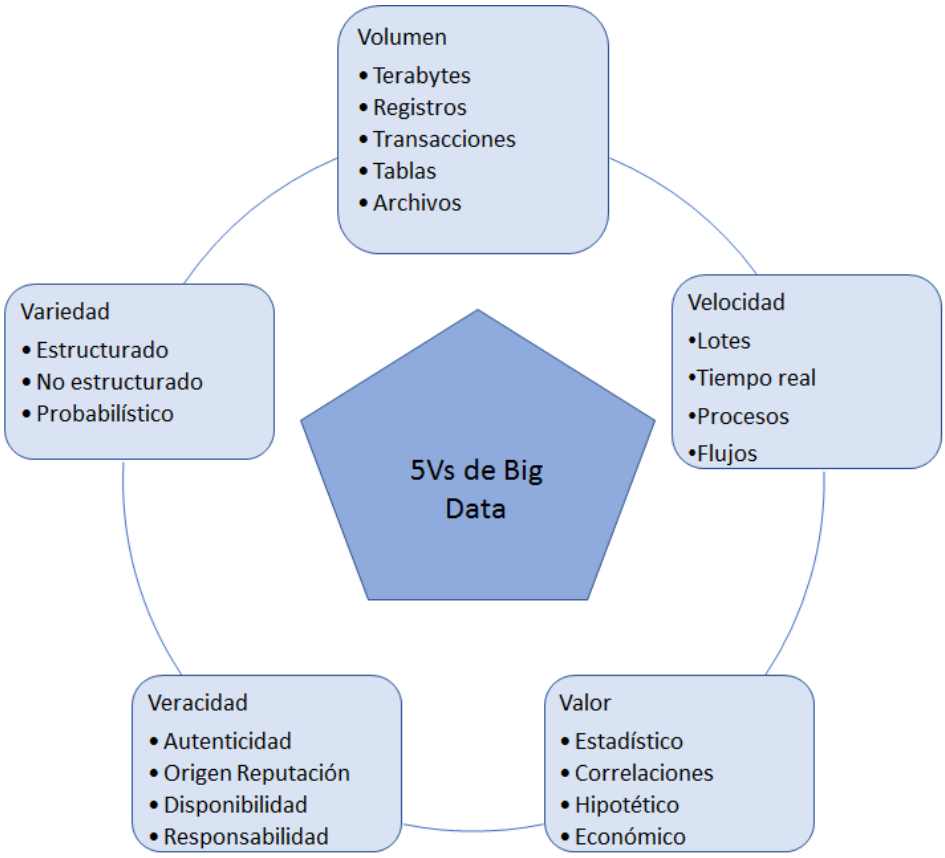

Figura 1: 5V´s de Big Data

Fuente: Modificada de Shaqiri, Bledi[4].

1) Volumen: se trata de gran cantidad de datos que disponen las empresas para analizar según sus respectivos objetivos.

2) Velocidad: se trata de la velocidad en la cual se generan los datos. Algunos autores hablan de un volumen que puede llegar a Peta bytes de datos generados diariamente. Dicha velocidad datos va en aumento debido a la interconexión de todos los dispositivos y al mundo globalizado e interconectado en el que vivimos.

[4] Shaqiri, Bledi. (2017). Exploring Techniques of Improving Security and Privacy in Big Data. 10.13140/RG.2.2.23201.10089.

3) Variedad: como se ha mencionado anteriormente, existen muchos tipos de fuentes de información. Tanto como las fuentes como, la variedad de datos es amplia, y va aumentando cada vez más a lo largo del tiempo.

4) Veracidad: Este parámetro de las V´s resulta de gran importancia ya que sería el más relevante. A parte de evitar la desinformación, se trata de que los datos generados sean veraces, para que así el resultado que se obtenga sea de acorde con la realidad.

5) Valor: este aspecto hace referencia a la relevancia de los propios datos, a la utilidad o beneficio que obtienen de ellos sus propietarios al explotarlos

Estas 5 V´s son la base en la cual se fundamentan el concepto de Big Data y que marcan el ritmo de este mismo.

3 LA PROTECCIÓN DE DATOS COMO REFLEJO DE LOS DERECHOS CON EL *BIG DATA*

El internet de las cosas y el *Big Data* se ha convertido en una realidad en nuestro día a día, por ello, la tecnología ya no es un problema. Comienzan así, una serie de incertidumbres morales y éticas: ¿cómo usamos los datos y con qué fin? Es decir, con que uso ético se plantea el uso de la información personal. ¿A qué riesgos nos estaríamos enfrentando como particulares? Ya que estamos exponiendo nuestros datos. Pero ¿Existe algún tipo de control sobre estos? ¿Cedemos en cierta manera nuestros datos, sin que se nos explique qué fin tiene ese uso?

Toda la información que compartimos en internet, con quién hablamos en nuestras redes sociales, dónde y con qué nos movemos (geolocalización móvil y reconocimiento facial), hasta nuestra solvencia financiera, son usados con distintos fines y pueden ser usados de

manera que se utilicen para agrupar y asignar un valor o un "rating" a cada ciudadano[5]. De esta manera, se controla por ejemplo la publicidad que se le enseña, dependiendo de dicho "rating" o valor que se la ha añadido específicamente.

Aunque parezca algo que en un principio suena a ciencia ficción es algo que se está empezando a aplicar e incluso a mover grandes sumas de dinero. Un ejemplo de ello es el claro caso de "*Facebook*" o "*Google*", que permitía el uso de sus datos, es decir de todos sus usuarios para que mediante una empresa ajena llamada "*Cambridge Analytics*" se influenciaran supuestamente dichos usuarios de manera que se decanten por una opinión política.

Lógicamente aquí se empieza a vulnerar un derecho. Un derecho que en un principio es el **derecho de privacidad**. Un derecho reconocido en numerosas constituciones y recogida en el artículo 18 de la constitución española y en la Carta de los Derechos Fundamentales de la Unión Europea.

"Artículo 18 – Derecho

Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.

2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito."[6]

De este artículo de la constitución cabe destacar el concepto de intimidad personal y familiar al igual que la propia imagen. De la misma manera existe una mención en el artículo 8.1 de la Carta de los Derechos Fundamentales de la Unión Europea.

"Artículo 8.- Protección de datos de carácter personal

1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.

2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a obtener su rectificación.

[5] Berinato, S. (2014). With big data comes big responsibility. *Harvard Business Review*, *92*(11), 20.

[6] Constitución española de 1978. «BOE» núm. 311, de 29/12/1978, Referencia BOE-1978-31229.

3. El respeto de estas normas estará sujeto al control de una autoridad independiente."[7]

Al ser tratado como un derecho fundamental, existe por tanto una regulación a nivel europeo, e internacional. Por ello, y como prueba de que dicha vinculación entre distintos derechos como los de privacidad, e intimidad, existe, se crea un marco general legal, de manera que se garantice dichos derechos y exista incluso hasta distintas sanciones de manera que un quebrantamiento tenga consecuencias legales.

4 REGULACIÓN

4.1 Regulación a Nivel Estatal y Europea

Existe una protección que se da al uso de los datos, de manera que se reconoce un derecho fundamental reconocido en la Constitución Española en el articulo 18. Dicho artículo está contenido en la Sección 1ª, del Capitulo II del Título I de la Constitución Española, de ese modo se garantiza el **derecho al honor, a la intimidad personal y familiar y la propia imagen**. Lo que es relevante de dicho artículo es el apartado 4: "*la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de lo ciudadanos y el pleno ejercicio de sus derechos"*.[8]

De esta manera, se regula la Protección de Datos y se representa como un derecho fundamental de la sociedad española. El hecho que se considere como tal, provoca que se regule estos mismos mediante la Leyes Orgánicas.

Para ello, el 13 de diciembre de 1999, entró en vigor la Ley Orgánica 15/1999, la cual establecía la protección de datos de carácter personal y será de aplicación siempre y cuando no entre en conflicto con la conocida RGPD[9].

Este último es un reglamento publicado por la Unión Europea en mayo de 2016, y que no entró realmente en vigor hasta el 10 de mayo del 2018. Este busca en un primer momento

[7] Carta de los Derechos Fundamentales de la Unión Europea, Diario Oficial Nº. C. 303, de 14/12/2007.

[8] Constitución española de 1978. «BOE» núm. 311, de 29/12/1978, Referencia BOE-1978-31229.

[9] REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016.

establecer el derecho de protección de datos, y todos aquellos derechos que busca proteger como un derecho fundamental. De manera que estos derechos, tiene alcance general mediante el RGPD. Esto significa que según el articulo 288 del Tratado Fundamental de la Unión Europea (TFUE), no se requiere un acto de transposición por parte de ninguno de los Estados miembros para aplicar dicho reglamento de la Unión Europea.

De nuevo, la Ley Orgánica 15/1999 del 13 de diciembre de 1999, adapto al ordenamiento jurídico español las disposiciones recopiladas en la Directica 95/46/CE del Parlamento Europeo y del Consejo Europeo de 1995. Estas directivas buscan la protección de las personas físicas en todo aquello que haga referencia al tratamiento de datos personales y a la libre circulación de estos mismos.

En los artículos relevantes del reglamento encontramos el articulo 3, el cual establece:
"ARTÍCULO 3
La Directiva 95/46/CE del Parlamento Europeo y del Consejo (4) trata de armonizar la protección de los derechos y las libertades fundamentales de las personas físicas en relación con las actividades de tratamiento de datos de carácter personal y garantizar la libre circulación de estos datos entre los Estados miembros.[10]"
Es decir, que este establece en un primer momento el ámbito de aplicación territorial. De modo que busca armonizar dicha protección de derechos y libertades fundamentales de las personas físicas en relación con las actividades de tratamientos de datos.

Otro artículo de relevancia de dicho reglamento es el Artículo 7 de este.
"Artículo 7
Estos avances requieren un marco más sólido y coherente para la protección de datos en la Unión Europea, respaldado por una ejecución estricta, dada la importancia de generar la confianza que permita a la economía digital desarrollarse en todo el mercado interior. Las personas físicas deben tener el control de sus propios datos personales. Hay

[10] REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016.

que reforzar la seguridad jurídica y práctica para las personas físicas, los operadores económicos y las autoridades públicas."[11]

Mediante este artículo se pone énfasis, en la importancia de la protección de datos. Debido a que existe un aumento de flujos transfronterizos de datos personales entre los distintos miembros de la Unión. Además, dicho aumento de estos flujos está acompañada de una evolución rápida en términos tecnológicos y una globalización cada vez mayor. De esta manera, la Unión Europea busca hacer frente a la utilización del Big Data y hacer frente a sus distintos fines, ya sean tanto públicos (por ejemplo, en sanidad) o privados (por ejemplo, económicos), y tener asido un marco jurídico más sólido, más protector, y más coherente.

No cabe olvidar también la aprobación a nivel nacional, del Real Decreto- ley 5/2018 del 27 de julio de medidas urgentes para que el derecho y la normativa europea se aplicase al derecho español, en todos aquellos aspectos que no representen un derecho fundamental (por lo que recordemos que no requiere una Ley Orgánica). De esta manera se garantiza en la mayor medida de lo posible la aplicación del Reglamento 2016/679, del Parlamento Europeo y del Consejo del 27 de abril de 2016.

Finalmente llego a España la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales[12]. Esta Ley Orgánica busca modificar las exigencias en cuanto al tratamiento de la información personal tanto de usuarios como de empresas ya sean empresas o usuarios. De esta manera, al igual que a nivel europeo, se busca en España establecer un marco legislativo en cuanto a la protección de datos personales en Internet. Garantizando así, nuevos puntos a tener muy en cuenta como el Derecho al olvido o a la portabilidad, al igual que modificaciones en cuanto a las condiciones a tener en cuenta respecto del consentimiento, y del propio uso que se realiza de los datos en cuestión.

[11] REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016.

[12] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales., Referencia: BOE – A – 2018 -16673

La Ley Orgánica 3/2018, buscó modificar la antigua ley mencionada anteriormente de Protección de datos de (1999).

Mediante esta figura se esquematiza las novedades y las modificaciones de la RGPD:

Figura 2: Novedades de la RGPD

Fuente: Tablado F[13].

4.2 ¿Qué Consecuencias tiene a nivel digital?

El Reglamento 2016/679, del Parlamento Europeo y del Consejo refuerza en muchos aspectos la protección digital de manera que esta se vea cada vez más reforzada. Para ello se establecen una serie de condiciones, para así proteger a los usuarios y así el derecho fundamental de la privacidad innato a cada uno de ellos, frente a los riesgos que puede acarrear el mundo digital como seria la suplantación de identidad o el abuso publicitario, también conocido coloquialmente como *spamming* "*SPAM*".

Estas condiciones se pueden resumir en:

[13] F Tablado F. Ley de Protección de Datos y Garantía de Derechos Digitales (LOPDGDD) 2018. (Disponible en: https://protecciondatos-lopd.com/empresas/nueva-ley-proteccion-datos-2018/; última consulta 15/02/2021)

- El consentimiento debe siempre existir y estar presente en todo momento, de manera que este sea a parte de lógicamente expreso, sea también verificable por parte del usuario.
- La obligación de informar la identidad de la entidad encargada del tratamiento de los datos, incluso si la gestión de la información es cedida a terceros.
- La obligación de informar al usuario que es lo que se va a hacer con la información, durante cuanto tiempo va a estar almacenada, al igual que donde.
- La obligación de dar la posibilidad al usuario de recuperar su información al igual que solicitar todo tipo de dato y/o información que se tenga sobre el.
- La obligación de otorgar al usuario el "derecho de olvido", mediante el cual el usuario puede limitar y prohibir el uso de los datos que tenga la identidad. Este derecho se permite revocar un consentimiento otorgado previamente. A pesar de ellos el "derecho al olvido" tiene una serie de requisitos para proceder a su eliminación, y esta debe ser que la información en cuestión no esté actualizada, y/o que no se sea pertinente al igual que sea excesiva.
- En todo momento, se debe de informar el marco jurídico empleado

Estas son unas de las condiciones que se imponen en cuanto al tratamiento de la privacidad digital, de manera que, si no se cumplen, puede llevar consecuencias legales, e incluso penales para ciertos casos.

En un primer momento, es decir, incluso antes de la aplicación del RGPD, ya había un especial cuidado y precaución con el uso de los datos que se realizaban. Se debía a que muchos datos podían ser de gran sensibilidad, como por ejemplo la orientación sexual del usuario, su orientación política, preferencias ideológicas, o su religión.

En un primer momento, se entiende que dichos datos, o agrupaciones de datos en cierta manera parecen irrelevantes. ¿De verdad tiene alguna relevancia saber la orientación ideológica de una persona para saber sus preferencias en cuanto a zapatillas? En un primer momento lógicamente, no tiene ningún tipo de relevancia. Sin embargo, resulta de gran importancia si de alguna manera queremos influenciar un grupo de usuarios para que voten o no voten a un partido en cuestión. Este fue el grave caso que ocurrió durante el Brexit. Durante la campaña a favor y en contra del Brexit, se hostigó a los usuarios indecisos con publicidad política de manera que se decantaran, por un lado, y así no tengan una decisión imparcialmente tomada.

4.3 Posibles sanciones y recursos

Una de las primeras consecuencias que hubo con el Reglamento Europeo que entró en vigor, fue de establecer sanciones económicas que pueden ascender hasta los 10 millones de euros. Por ejemplo, el caso del Brexit, el cual se analizaron datos de carácter privativo para conocer la orientación sexual, su ideología política y/ o religión.
Este régimen jurídico sancionador viene recopilado en los artículos 77 a 84 del RGPD. Se plantea los posibles recursos, como las responsabilidades y sanciones de aquellas personas físicas y jurídicas que realicen un quebrantamiento de los derechos en cuestión. Se plantea una serie de **reclamaciones** para proteger los derechos de los interesados respecto de los responsables del quebrantamiento:

- *"Derecho para presentar reclamaciones, a las distintas autoridades de protección de Datos en el Estado miembro en el cual se encuentre el individuo, el propio lugar de trabajo o el lugar de la infracción. Cabe también mencionar que se incluye el recurso en caso de que la Autoridad de Protección de Datos no aborde la reclamación".*[14]

- Se proporciona el derecho a recurrir las distintas decisiones que sean de carácter vinculante que hayan sido emitidas por las Autoridades de Protección de Datos. Ese derecho de recurrir se permite realizarlo ante los tribunales nacionales. Por ello, se permite iniciar procedimientos judiciales ante tribunales nacionales.

¿Pero qué ocurre con todo lo referido a la responsabilidad de los infractores?
Para ello se establece una serie de responsabilidades y unas determinadas sanciones. Estas sanciones y/o indemnizaciones dependerán de la gravedad de la infracción cometida. Tanto la LOPD/RLOPD (régimen antiguo), como el RGPD (nuevo régimen), contemplan

[14] Serrano A. Big Data y protección de datos. (Disponible en https://www.antonioserranoacitores.com/big-data-proteccion-datos/#312_Recursos_responsabilidad_y_sanciones; última consulta 15/03/2021)

distintos tipos de sanciones, de nuevo dependiendo de la gravedad de la infracción[15].

Norma aplicable	Sanciones		
LOPD/RLOPD	Leve	Grave	Muy grave
	900€ - 40.000€	41.001€ - 300.000€	300.000€ - 600.000€
RGPD	No se establece un rango mínimo de cuantía.	Multa administrativa de hasta 10 millones de euros o, en el caso de empresas, de cuantía equivalente al 2% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, lo que resulte mayor en cuantía.	Multa administrativa de hasta 20 millones de euros o, en el caso de empresas, de cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, lo que resulte mayor en cuantía.

Tabla 2: Nuevo Régimen Sancionador del RGPD, comparado con el anterior LOPD/RLOPD

Fuente: Serrano A[16].

Se puede observar que el régimen sancionador, y las sanciones y/o indemnizaciones contempladas se han endurecido drásticamente, de manera, que un ataque a los derechos protegidos por el reglamento podría suponer el fin de muchas empresas, que serían incapaces de hacer frente a las sanciones del Reglamento.

También cabe mencionar que estas sanciones son independientes de que los Estados miembros de la Unión Europea puedan imponer a parte, sanciones de carácter económico y/o administrativas, e incluso imponer sanciones de carácter penal. Por ello, el régimen sancionador que se establece en el nuevo RGPD, demuestra la gran relevancia que se le está dando a la protección de los derechos fundamentales, mucho mayor que en el anterior régimen.

[15] Puig, A. R. (2018). Daños por infracciones del derecho a la protección de datos personales. El remedio indemnizatorio del artículo 82 RGPD/Liability for Data Protection Law Infringements. Compensation of Damages under Article 82 GDPR. *Revista de Derecho Civil*, *5*(4), 53-87.

[16] Serrano A. Big Data y protección de datos. (Disponible en https://www.antonioserranoacitores.com/big-data-proteccion-datos/#312_Recursos_responsabilidad_y_sanciones; última consulta 15/03/2021)

5 LOS MECANÍSMOS DE GOBIERNO DEL NUEVO RÉGIMEN RGPD

Para evitar este tipo de sanciones, se establece una serie de mecanismos en el RGPD en busca de realizar un control, sobre el cumplimiento correcto que se hace de los datos.

Para ello, el RGPD incorpora unas serie de novedades con respecto a un sistema de control con el fin de gobernar con un correcto funcionamiento ético en cuanto a la protección de datos.

Estas novedades se ven reflejadas entre los artículos 24 y 25, 32, 35, 37, 40 y 42 del RGPD, estos artículos versan sobre la creación, bajo una forma obligatoria, de medidas en los programas para que se garantice el cumplimiento del RGPD. Sobre todo, para aquellos casos en los cuales se busque demostrar ante las autoridades o ante cualquier individuo interesado en el buen funcionamiento del RGPD. Estas implementaciones pueden ser varias, desde la implementación de políticas de protección de datos hasta incluso técnicas para su correcto funcionamiento.

5.1 Políticas de protección de datos

Se trata de todas aquellas políticas implementadas por la empresa. Por ello, es una implementacion característica de la nueva regulación del RGPD, por el que se trata de solucionar el riesgo de que en una misma empresa trate de forma distinta los diferentes aspectos de la RGPD[17]. Por lo que implementar una política de protección de datos de manera uniforme por una misma empresa entre sus distintos departamentos es fundamental. Sin embargo, se trata de una medida de control que es optativa por lo que no tiene un carácter obligatorio para las empresas.

[17] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal

5.2 Códigos de conducta

Este aspecto viene regulado en los artículos 40 y 41 del RGPD, en la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (LOPDPGDD). Art 38 y disposición transitoria segunda), al igual que en las Directrices 1/2019 del Comité Europeo de Protección de Datos (CEPD)[18].

El código de conducta se podría definir como un conjunto de normas elaboradas por la empresa u organización en cuestión, con el fin de definir de regular el comportamiento de los miembros de esta. Estas normas de conducta además, no estan exigidas en ningún momento por ningun tipo de ley ni de disposición administrativa.

Estos códigos de conducta a diferencia de otras medidas, son optativas, es decir no tienen porque realizarse siempre[19]. Sin embargo, al igual que para las Políticas de Protección de Datos, existe una finalidad probatoria por parte de los códigos de conducta con respecto de las autoridades que pueden ser tanto estatales como supranacionales. Entre ellas pueden ser tanto la Comisión Ética Española, como el CEPD.

Estos Códigos de Conducta buscan versar sobre distintos aspectos como el tratamiento leal y transparente que se hacen de los datos, los intereses legítimos perseguidos, la recogida de los datos personales, la información proporcionada al público y a los interesados, etc. Al no existir una lista cerrada o de *numerus clausus*, no se define en un sentido cerrado el contenido en el que tiene que versar, las opciones son muy variadas y al final se deja un poco a la autonomía de la propia empresa en cuestión. Sin embargo, todo aquello que se regule tiene un carácter vinculante para los miembros de la empresa y por ello, su contenido se convierte en obligatorio para los responsables o aquellos que esten adheridos al propio código de conducta.

Esta diferencia provoca en cierta manera que no se regule unitariamente un aspecto de gran relevancia a nivel ético ya que no establece ningun tipo de problema en el caso que

[18] Auñón, N. R. (2019). Los códigos de conducta y las certificaciones en el RGPD (Arts. 40-43 RGPD. Arts. 38-39 y Disposición transitoria segunda LOPDGDD). In *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD* (pp. 549-568). Wolters Kluwer.

[19] Bennett, C. J. (1992). *Regulating privacy: Data protection and public policy in Europe and the United States*. Cornell University Press.

no se haya tratado un aspecto. Es decir, el Código de Conducta puede no tratar algunos aspectos que una empresa son de gran importancia.

Supongamos que un Código de Conducta no ha regulado claramente o con precisión un aspecto del buen comportamiento ético. ¿Qué ocurre? ¿Se tiene que cumplir todo lo claramente establecido por el código de conducta salvo ese aspecto determinado? Esto genera en cierto aspecto un sentimiento de incertidumbre y de desconfianza para los usuarios por lo que no queda claro qué se pude hacer y no hacer. Por ende, se puede tener comportamientos poco éticos que no queden definidos en el propio Código de Conducta.

El hecho que no quede perfectamente definido un comportamiento ético de manera cerrada, puede llevar a cabo por las empresas a saltarse esa moral, y que además no exista una reprimenda como tal ante un incumplimiento de este. Esto, deja mucho que desear en este tipo de control. Parece que aún queda mucho camino por recorrer en cuanto a la regulación de este tipo de control.

Sin embargo, a pesar de no existir un control negativo ante el incumplimiento de este tipo de control , existe un control positivo, en el sentido que se insta a las empresas a aplicar correctamente el RGPD, facilitando y adecuando asi su aplicación. De esta manera, se entiende que el código de conducta sirve como, por ejemplo, demostración del correcto cumplimiento de las obligaciones de los distintos resopnsables y encargados de la empresa. De la misma manera, en caso de existen posiblas sanciones por el incumplimiento del RGPD, se tiene en cuenta el Código de Conducta de manera a que las sanciones sean mas laxas.

5.3 Mecanismos de certificación

Al igual que para los Códigos de Conducta, el RGPD contempla una serie de mecanismos de certificación de manera que, de la misma forma que los códigos de conducta y de las Políticas de Protección de Datos, tienen un efecto probatorio.

Además, se establecen una serie de criterios de certificación, los cuales deben estar aprobados por una Autoridad de Protección de Datos que tenga competencia al igual que por el propio CEPD.

Esta certificación además sigue un proceso mediante el cual se busca recabar toda la información posible y necesaria al respecto de los datos. Esta información será facilitada

por el responsable de la empresa y los encargados de la recopilación, tratamiento y análisis de los datos[20].

Una vez otorgado el certificado de los datos, es decir el "*Sello Europeo de Protección de Datos*", esta tendrá una validez de tres años, y se podrá renovar siempre y cuando cumpla con las mismas condiciones por las que se ha otorgado.

La concesión de la certificación por parte de las autoridades competentes genera una serie de efectos que hay que tener en cuenta y que son muy similares a los efectos que generan la realización de los Códigos de Conducta:

- Validez probatoria del correcto cumplimiento de las obligaciones de los responsables de la empresa en cuanto a la recopilación y tratamiento de datos
- Validez probatoria de todas las medidas de seguridad adecuadas para la recopilación de datos y tratamientos de estos mismos.
- Tiene un valor probatorio para demostrar que los responsables y todos aquellos encargados cumplen con las suficientes garantías a la hora de realizar transferencias internacionales de datos y cumplen correcta y adecuadamente con el RGPD.
- Al igual que para los Códigos de Conducta, tienen un valor beneficioso en el caso que se aplican sanciones por infracciones a la Protección de Datos. Es decir, tienen un factor paliativo en el posible caso que se impongan sanciones a la empresa.

Se trata de un caso relativamente similar tanto a los Códigos de Conducta como a las Políticas de Protección de Datos. Sin embargo, aquí hay que destacar que a diferencia de los otros dos mecanismos de control que hemos visto por el momento, el mecanismo de certificación interviene una autoridad competente. Es decir, que el RGPD contempla y trae como novedad la creación de un organismo de certificación de manera a que se acredite correctamente los datos, y el buen funcionamiento y tratamiento que están haciendo de ellos en las empresas.

Uno de los objetivos principales de este tipo de certificaciones como el "*Sello Europeo de Protección de Datos"* es también de dar un aspecto de confianza a los usuarios, es decir aquellos que tengan certificaciones otorgados por la autoridad con competencia

[20] Lachaud, E. (2018). The General Data Protection Regulation and the rise of certification as a regulatory instrument. *Computer Law & Security Review*, *34*(2), 244-256.

generaran una situación de garantía para los usuarios de los datos. De esta manera, se convierte en un argumento que tiene un valor competitivo.

No obstante, la obtención de estas certificaciones o sellos tienen un **carácter voluntario** que está acompañado en cierta medida con una serie de efectos positivos, por ejemplo, ante una posible sanción económica a la empresa por una vulneración de derechos en cuanto a la protección de datos, se estipula que solo podrá ser impuesta en los casos de incumplimiento intencionado o negligente. Se recuerda que las sanciones pueden llegar a ser de una cuantía de 100.000.000 de euros o el cinco por ciento de su volumen de negocios.

5.4 Seudonimización de datos

La antigua Ley Orgánica de Protección de Datos, presentaba ya una regularización de un proceso similar a la seudonimización de los datos. Este recogía y regulaba el proceso conocido como la anonimizacion de los datos, pero con la entrada en vigor del RGPD se dio lugar a la seudonimización de los datos[21].

Estos aspectos vienen regulados también tanto a nivel europeo como a nivel nacional:

-"*A nivel europeo:*

- *RGPD*
- *Dictamen 05/2014 del Grupo de Trabajo 29*

-A nivel nacional:

- *Nueva Ley Orgánica de Protección de Datos y de Garantía de Derechos Digitales*
- *Ley 14/2007, de 3 de julio, de Investigación Biomédica*"[22]

En primer lugar, se distingue el concepto de anonimización o disociación de datos personales con la seudonimización, de manera que se entienda la novedad que aporta. La anonimización se trata de romper el vínculo que existe de manera total entre los datos personales que vamos a tratar con los datos que hemos identificados. De esta manera impedimos asociar cualquier tipo de dato a una persona en concreto, y así identificarla.

De esta manera, se busca la imposibilidad de que exista ningún tipo de asociación de datos con los datos identificativos o personales de la persona o del individuo en cuestión.

[21] Ortigosa, A. P. (2019). Decisiones automatizadas en el RGPD. El uso de algoritmos en el contexto de la protección de datos. *Revista general de Derecho administrativo*, (50).

[22] González, Y. (2020, 24 abril). *La seudonimización y anonimización de datos personales*. Grupo Atico34. https://protecciondatos-lopd.com/empresas/seudonimizacion-anonimizacion/#Normativa

Por otro lado, en cuanto a la seudonimización, el artículo 4 de la RGPD establece lo siguiente:

"[...] aquella información que, sin incluir los datos denominativos de un sujeto, permiten identificarlo mediante información adicional, siempre que ésta figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.[23]*"*

De esta manera, en vez de romper el vínculo se realiza un tratamiento de los datos de manera que se cambian los datos personales de un usuario, pero sin tener los datos identificativos del interesado. Se suprime así, el vínculo que permite conectar los datos a un individuo o persona en concreto. Un ejemplo de ello sería la sustitución de nombres, por un código aleatorio o identificador numérico. En otras palabras, se cambian o se sustituyen los datos personales de cada individuo por seudónimos.

De nuevo, la seudonimización tiene una finalidad similar a la anonimización, pero al realizar un procedimiento diferente mediante sustitución, se pretende minimizar en todo lo posible, que el usuario o individuo en cuestión sea identificado. Realmente se busca determinar la protección de la información adicional de manera que sea esta la que pueda identificar a el individuo.

De nuevo, se denota otra vez el problema de que **no tiene un carácter coercitivo**. Es decir, no es obligatorio en ningún momento llevar a cabo al seudonimización y/o anonimización de los datos personales. Por lo que de nuevo se tiene una cierta confusión en cuanto a los alcances del RGPD. No queda claro en ningún momento las posibilidades en cuanto al uso que se puede hacer de los datos y los límites que se le ponen a eso.

Es decir, la importancia de la seudonimización y/o la anonimización de los datos en cierta manera conservar una figura de anonimato por parte de los individuos, y que estos no se vean en cierta manera identificados. Este tipo de control suele darse sobre todo en ámbito sanitario y farmacéutico, ya que se separa el elemento identificativo del individuo para quedarse con los datos relativos al estudio en cuestión.

No obstante, parece que es algo de crucial. El hecho de poder anonimizar los datos tiene que ser fundamental para el tratamiento de datos en internet y en el *Big Data*. El hecho de poder navegar en la web, y que el *Big Data* afecte de una manera u otra a nosotros no significa que las empresas en cuestión tienen que saber nuestros datos personales. Por

[23] REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016.

ello, la privacidad es garantizada en gran medida por la anonimización o seudonimización de los datos, y al no existir una vertiente coercitiva del RGPD, no se garantiza dicho derecho a la privacidad.

5.5 Minimización de datos

La nueva normativa que plantea la RGPD específicamente en el artículo 4, en concreto en el apartado 1.c) establece una serie de principios generales en cuanto al tratamiento de datos[24]. En específico, se hace referencia al principio de minimización de datos:

"Artículo 4: Principios relativos al tratamiento

1. *Los datos personales serán:*
    a. *Tratados de manera lícita, leal y transparente en relación con el interesado ("licitud, lealtad y transparencia");*
    b. *Recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales ("limitación de la finalidad"):*
    c. *Adecuados, pertinentes y limitados a lo necesario en la relación con los fines que son tratados ("minimización de datos");*
    d. *Exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines que se tratan ("exactitud")"*[25]

[24] Heuer, H., & Breiter, A. (2018). Student success prediction and the trade-off between big data and data minimization. *DeLFI 2018-Die 16. E-Learning Fachtagung Informatik*.

[25] REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016.

Por ende, se analiza la definición que da el RGPD a la minimización de datos puede establecer una serie de requisitos:

- Solo se puede recabar la información o los datos personales que se vayan a usar, es decir, se exige que solo se recopilen los datos necesarios que se van a utilizar por parte de los usuarios.
- Se establece un requisito temporal, mediante el cual el requisito de la recopilación de los datos se debe hacer cuando se vaya a realizar el análisis en sí. Es decir, en otras palabras, no se puede recopilar la información o los datos personales de los usuarios y/o individuos en cuestión para realizar el tratamiento después.
- En último lugar, se plantea un requisito en cuanto al fin o el objetivo que se le van a dar a los datos. La utilización que se de los datos recopilados debe ser el mismo uso para el cual fueron recopilados en una primera instancia.

La minimización de datos tiene, por ende, una serie de consecuencias por las cuales se ven afectados tanto los usuarios como las empresas. Los usuarios en un primer principio son el objetivo de protección del RGPD, de manera que han establecido entre otras medidas, la minimización de datos de forma que limiten la forma o la manera que tienen las empresas de obtener la información en cuestión[26]. De esta manera se garantiza un derecho de acceso, rectificación, supresión, la limitación del tratamiento al igual que la portabilidad y la oposición (derechos que trataremos más adelante).

La minimización otorga al usuario un mayor poder de control sobre su información personal que tienen las empresas. De esa manera, los usuarios o individuos sabrán en todo momento cuanto tiempo, con que finalidad y cuando se recogen sus datos, de manera que aumenta la confianza que estos tengan cuando cedan sus datos y/o información personal a las empresas. [27]

Por otro lado, en cuanto a las compañías u organizaciones, el mecanismo de control que brinda el RGPD, mediante la minimización de datos, obliga a las empresas a replantear

[26] Goldsteen, A., Ezov, G., Shmelkin, R., Moffie, M., & Farkash, A. (2020). Data Minimization for GDPR Compliance in Machine Learning Models. *arXiv preprint arXiv:2008.04113*.
[27] Zarsky, T. Z. (2016). Incompatible: the GDPR in the age of big data. *Seton Hall L. Rev.*, *47*, 995.

los procesos de recopilación y tratamiento de datos de los usuarios. En esta faceta, además entra en juego la cuestión del consentimiento por parte de los usuarios, es decir la manifestación expresa y voluntaria por parte de los usuarios a ceder los datos, según sus propias condiciones para el tratamiento de estos por las empresas.

A diferencia de los otros tipos de mecanismos vistos hasta el momento, la minimización de los datos es obligatoria. Es decir, sí que tiene un carácter coercitivo implantado por el RGPD. Lógicamente, esto otorga una protección mayor a los derechos que se vulnerarían en caso de que no se cumpla con este mecanismo de control.

Es decir, la minimización es un primer mecanismo de control del RGPD donde aparecen y donde manifiestan estos derechos. La manifestación del principio del consentimiento es fundamental para entender el principio y que no se vean vulnerados otros derechos relativos a la privacidad individual.

5.6 Delegado de protección de datos

Una de las novedades más importantes que aporta el RGPD, es la creación de una nueva figura: el delegado de Protección de Datos o en inglés "*Data Protection Officer*". Se designa teniendo en cuenta sus cualidades profesionales y en particular sus conocimientos especializados en derecho en cuanto a la materia de Protección de Datos. El delegado se encarga de una serie de funciones, que dependerán lógicamente de la empresa para la que trabaje. Existen una serie de funciones mínimas establecidas en el RGPD:

- Iinformar y asesorar a la empresa o al responsable de esta en cuanto al tratamiento que se realice de los datos, y de aquellas informaciones y obligaciones que incumben el cumplimiento del RGPD.
- Supervisar el cumplimiento de todas las disposiciones que contenga el Reglamento, al igual que de otras disposiciones que vengan establecidas en otros reglamentos de los estados miembros.
- Asesorar en cuanto a la protección de datos y de todos aquello que venga relacionado o dispuesto en el artículo 35 del RGPD.
- Cooperar e informar con la autoridad de control

Por todo ello, tanto el RGPD[28] como el LOPD[29], presentan en ambos casos atención a la posición del delegado de Protección de Datos, "*con el fin de garantizar que pueda desempeñar su función libre de injerencias y sin someterse a instrucciones de la organización en la que presta servicio"* (Francisco Martínez Vázquez, 2019). De esta forma se busca evitar que exista ningún tipo de instrucción al delegado o que este sea removido por la propia empresa, se manera en que esta ultimo incurriría en sanciones. Todo ello, viene regulado en el artículo 36 del RGPD, de manera que se evite de cualquier manera un fraude por parte de las empresas a este delegado.

El delegado de Protección de datos viene estipulado en el artículo 37 del RGPD, por el cual, se define de manera amplia sus cargos y sus funciones. Para ello, la Ley Orgánica 3/2018, de Protección de Datos y Garantía de los Derechos Digitales, trata en el artículo 34, una serie de supuestos mínimos en los que es obligatorio designar el cargo de delegado de Protección de Datos. Por ejemplo, *"centros docentes que ofrezcan enseñanzas en cualquiera de los niveles establecidos en la legislación reguladora del derecho a la educación, así como las Universidades públicas y privadas, entidades que exploten redes y presten servicios de comunicaciones electrónicas conforme a lo dispuesto en su legislación específica, cuando traten habitual y sistemáticamente datos personales a gran escala, etc."*[30]

En cierta manera, se finaliza con la incertidumbre ya que se establece un mecanismo de control personal para ciertas materias en las cuales la protección de datos tiene gran importancia. De esta forma, se aplica una obligación a las empresas y que exista un control sobre el uso y la forma que se está teniendo de los datos.

---

[28] 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*). *Diario Oficial de la Unión Europea,* L 119/1, de 4 de mayo de 2016.

[29] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, *Boletín Oficial del Estado* no 294, de 6 de diciembre de 2018.

[30] Martínez Vázquez, F. (2019). "El reciente marco de la protección de datos personales (RGPD y nueva LOPDP): las obligaciones del responsable y del encargado el Delegado de Protección de Datos y el régimen sancionador".

Por otro lado, además el artículo 24 del RGPD, hace una mención a los Códigos de Conducta o a los mecanismos de certificación, de manera a que se otorga la posibilidad al responsable del tratamiento de datos o a el encargado, es decir, al delegado de Protección de Datos a adherirse a códigos de conducta de la propia empresa y que este pueda demostrar su correcto cumplimiento.

6 PRINCIPIOS ÉTICOS Y MORALES QUE PLANTEA

6.1 Consentimiento (Artículo 7 y 8 del RGPD)

A lo largo de la regulación, tanto europea como nacional, aparece constantemente tanto en Reglamentos, en Leyes Orgánicas como en Directivas, el **principio del consentimiento** que se trata como la manifestación de la voluntad inequívoca y expresa sin vicios a dar o no dar sus datos personales.

Por ello, el avance de las nuevas tecnologías, como en los teléfonos móviles, el internet de las cosas, distintos servicios de localización, etc. provoca que la manifestación del consentimiento sea más difícil de reconocer y de obtener.

La solución que se ha encontrado a dicho problema ha sido las políticas de privacidad online, es decir se tratan de contratos unilaterales y casi contractuales. Se basa la aceptación del individuo a consentir el tratamiento de sus datos, mediante la voluntad de firmar o de aceptar dichos contratos. Hoy en día, es el método, o la base en la que todas las empresas obtienen los datos de sus usuarios para tratar esos datos según las funciones que tengan.

Sin embargo, la realidad es otra ya que la gran mayoría de las personas no leen ni atienden a lo que están aceptando. Cuando una persona navega en la web, no se para cada minuto, o cada vez que entra en una página a leer y entender que se van a hacer con sus datos de navegación, o por ejemplo a dónde va a llegar la codificación de nuestra huella que tienen nuestros propios dispositivos móviles.

Ante esta situación, se obtiene en cierta manera un contrato inválido, ya que el consentimiento no está siendo claro, ni específico puesto que las personas realizan esa aceptación como un proceso que tiene el mundo de Internet.

Por ello, los distintos operadores jurídicos han demandado mejoras en lo relativo a:

- *"La forma en la que las políticas de privacidad son redactadas, de modo que haya una notificación efectiva; y*
- *Desarrollar mecanismos que permitan otorgar un consentimiento informado, con una especial importancia sobre los sistemas denominados opt-in y opt-out"*[31]

Para ello, existen muchas formas o procesos que se han realizado de manera a solucionar este problema, una de ellas es la simplificación del lenguaje. Mediante un lenguaje sencillo esto favorecía la comprensión de los usuarios de lo que implica la elección o la aceptación de la protección de datos. Sin embargo, no todo el mundo aboga por dicho procedimiento, ya que según Baroccas y Nissebaum[32], rechazan dicho concepto. Estos se basan en que a pesar de que los usuarios entiendan que es lo que está ocurriendo, estos no van a tener la información suficiente como para realizar un juicio de valor claro al respecto.

Un ejemplo de ello, sería la publicidad personalizada. Para tener la información suficiente, el usuario tendría que conocer: con quién se compartiría los datos, durante cuánto tiempo, que información se está recogiendo, etc. Por ello, al simplificar todo ello, faltaría información necesaria para el usuario para tomar una decisión consciente.

Por todo ello, todavía existe un gran dilema sobre el principio del consentimiento, y a pesar de la regulación exacta que nos brinda tanto el RGPD, como el LOPD, en cuanto a lo que es el principio de consentimiento en la protección de datos, no se encuentra una solución clara.

El hecho de que se manifieste el consentimiento del usuario de esta forma sigue siendo aun un tema que necesita desarrollo. Es necesario encontrar algún tipo de método para facilitar la comprensión total del usuario en cuanto a tomar la decisión de transmitir sus datos o no, de manera que quede claro.

[31] Gil González, E. (2015) "Big data, privacidad y protección de datos"

[32] Aleecia M. McDDONAL y lorrie FAITH CRANOR. "The Cost of Reading Privacy Plocies". *Journal of Law and Poolicy of the Information Sociaty, Vol. 4, nº3 (2008)*

6.2 Derecho a la portabilidad de los datos (Artículo 20 del RGPD)

El derecho de la portabilidad de los datos viene recogido en el RGPD como en otros dictámenes o reglamentos tanto europeos como nacionales (LOPD), es el derecho mediante el cual se permite al responsable del tratamiento de los datos, ya sea una persona física o jurídica a que este reciba o transmita a un tercero estos datos o al individuo en cuestión.

El RGPD buscó el derecho a otorgar más control a la persona física sobre que se está haciendo con sus datos, al igual que fomentar en cierta manera el Mercado Único Digital, ya que este derecho permite al interesado o al individuo en cuestión, a poder transferir o reutilizar sus datos personales con otras empresas.

Lógicamente, las implicaciones son que el interesado tiene derecho a reutilizar sus datos ya sea por sí mismo, o por otra empresa de manera que estos datos son exportados a la otra empresa para su uso. Sin embargo, el artículo 68 del RGPD, no obliga a la supresión de los datos por la otra empresa. (Eso correspondería al derecho al olvido que se expondrá más adelante)

No obstante, existen y se imponen unas series de limitaciones a dicho derecho. El RGPD, establece una serie de casos, en los cuales no será posible ejercer el derecho a la portabilidad.

- En primer lugar, se establece un límite en cuanto al origen de los datos y no se puede transmitir los datos inferidos por los originales. Es decir, solo se puede portar, o transmitir los datos originales y personales que facilitó en primera instancia el usuario o individuo. Todos aquellos datos que hayan sido inferidos o deducidos por el responsable de una empresa no serán objeto del derecho de portabilidad, tan sólo sólo aquellos que facilitó el individuo.
- No cabe el derecho a la oposición (derecho que se analizará mas adelante) en aquellos casos en los cuales, los datos en cuestión se refieran a terceros (siendo estas otras personas físicas)
- En el apartado 3 del artículo 20 del RGPD, se define el Derecho a la portabilidad y se establece claramente una de las condiciones legítimas para que exista dicho derecho. Este es el **consentimiento**, ya que si no se da el consentimiento, estos no

podrán ser objeto del derecho a la portabilidad. De esta manera, se manifiesta siempre la protección de la privacidad del individuo. Si este se negó, o no brindó el consentimiento por el cual se puede transmitir esos datos, estos no podrán hacerlo (y podrían ser incluso sujetos de sanciones).

- Por último, se hace referencia al momento en el que los datos estén anonimizados o suprimidos, no se podrá realizar la portabilidad de estos, ya que esto supondría la supresión de la protección que existe sobre los datos personales.

Las limitaciones que se dan en cuanto al derecho de la portabilidad resultan del principal objetivo del RGPD, la protección de la privacidad y de los datos personales de los usuarios. Como se ha podido comprobar, en todo momento se busca proteger aquellos datos que ha proporcionado el individuo, ya que en estos casos siempre media el consentimiento en cuanto a su portabilidad a terceros.
Además, el derecho de la portabilidad también brinda la opción al individuo de conocer en todo momento qué información se tiene sobre el por parte de la empresa. Esto es de gran relevancia, ya que permite al usuario conocer toda la información necesaria para entender la situación que puede tener con una empresa. De esta manera, el individuo puede tomar acciones de manera a que se supriman sus datos (derecho al olvido).

A nivel ético, el derecho de portabilidad es un gran avance, ya que favorece el mercado digital único, puesto que las empresas pueden pasarse información sobre los usuarios y realizar distintos tratamientos. La importancia del derecho de portabilidad siempre está conectada con el principio de consentimiento, de manera que el individuo siempre tiene la decisión final en cuanto al uso de sus datos. Además, la posibilidad que existe mediante el derecho de portabilidad, por el cual el individuo conoce u obtiene toda la información que se tiene de él, es de gran importancia. Sin embargo, no hay que olvidar, que el proceso mediante el cual se obtiene esa información es distinto en cada empresa, y en muchas casi inexistente a menos que te pongas en contacto con estos. Por ejemplo, en "*Google*", se puede acceder en todo momento a que información que tienen y que saben sobre los individuos, al igual que a quién le están dando esa información personal.

No deja de ser un Derecho que ha otorgado un gran avance a la regulación del *Big Data* y la protección de datos, pero sin embargo todavía tiene algunos matices que hay que

cubrir, como, por ejemplo, en cuanto a la obtención de la información personal, que difiere entre empresa y empresa.

6.3 Derecho al olvido o supresión (Artículo 17 del RGPD)

El derecho al olvido o el derecho a la supresión viene regulado en el artículo 17 del RGPD. Se trata de uno de los derechos nuevos que nos brinda el RGPD, y que tiene una gran relevancia con respecto al Big Data y a la protección de datos.

Al igual que otros derechos novedosos incorporados por el RGPD, este tiene el mismo objetivo, y es el de otorgar o proporcionar mayor protección y control a los usuarios sobre sus datos personales.

Este derecho brinda la oportunidad a los usuarios de que sus datos de la red o que estén en posesión de distintas empresas "desaparezcan" de sus sistemas.

De nuevo, existe una gran correlación entre el derecho al olvido o supresión con el principio del consentimiento, ya que este derecho permite al interesado en todo momento revocar el consentimiento inicial que dio para el uso de sus datos y solicitar así, que sus datos sean eliminados permanentemente. De la misma manera, existe, por ende, una gran conexión también con otros dos derechos, que son el derecho al honor, y a la intimidad.

La normativa relacionada con el derecho de olvido y la RGPD son:

- "*A nivel europeo, el RGPD*
- *A nivel nacional:*
    - *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*
    - *Real Decreto 1720/2007, de 21 de diciembre por el que se aprueba el reglamento de desarrollo de la LOPD*
    - *Ley Orgánica de Protección de Datos de Carácter Personal y Garantía de Derechos Digitales (LOPDGDD)"*[33]

[33] González, Y. (2021, 17 marzo). *Derecho al Olvido en el RGPD*. Grupo Atico34. (Disponible en: https://protecciondatos-lopd.com/empresas/derecho-olvido-rgpd/; última consulta 01/04/2021)

El artículo 16 del LOPD menciona el derecho de cancelación, se trata de un derecho distinto al derecho de olvido. Ya que no da lugar a la eliminación de forma permanente de los datos. El derecho de cancelación hace referencia a la suspensión del uso de los datos personales, permitiendo entonces la conservación de estos por la entidad en cuestión.

Figura 3: Esquema del Derecho al olvido, obligaciones del RGPD.

Fuente: Grupo Ático34[34].

Al igual que para otros derechos contemplados en la regulación (sobre todo la RGPD), existe una serie de limitaciones al derecho al olvido que, a diferencia del derecho al olvido, se basan en intereses públicos en vez de en el consentimiento, puesto que este tiene prioridad respecto del otro. En aquellos casos, como por ejemplo se trate de garantizar la libertad de expresión, de cumplir con obligaciones legales, o cuando su finalidad sea para investigación científica, histórica o estadísticas.

Por ello, existe un choque o un enfrentamiento entre el derecho a la información y el derecho al olvido. Ante el derecho de olvido, el único derecho que se puede alegar es el

[34] González, Y. (2021, 17 marzo). *Derecho al Olvido en el RGPD*. Grupo Atico34. (Disponible en: https://protecciondatos-lopd.com/empresas/derecho-olvido-rgpd/; última consulta 01/04/2021)

derecho a la información. Se traza esa limitación siempre que exista una relevancia pública y que exista un interés público, primara el derecho de información. Sin embargo, con respecto a toda aquella información personal que no resulte necesaria o que carezca de interés público será susceptible al derecho de supresión o de olvido.

El derecho al olvido o la supresión tiene una gran importancia, ya que permite eliminar en todo momento toda información con un carácter permanente. Como hemos dicho anteriormente esta correlacionado con el control que otorga la revocación del consentimiento brindado en un primer momento.

Lógicamente existe un proceso mediante cada usuario puede solicitar la revocación de los datos personales que tenga una empresa sobre este.

No obstante, sigue siendo difícil atender al proceso de manera clara, y muchas veces al no tener una conciencia clara de que datos están circulando en internet, es difícil ejercer el derecho al olvido. Es por ello, mucho más fácil eliminar los datos que tiene *Google* de nosotros o de cualquier portal, los cuales tienen un proceso claro y conciso a la publicación que hicimos hace 8 años en las redes sociales.

El derecho al olvido es un gran avance en cuanto a la protección de datos, y su regulación es algo necesario en cuanto a la aplicación de un sistema de control claro al usuario. De esta manera, el usuario tiene el control y la última palabra sobre que se hacen con sus datos y quien los tiene.

6.4 Derecho de oposición (Artículo 21 del RGPD)

Regulado en el artículo 21 del RGPD, el derecho de oposición es el derecho que permite al interesado en los distintos casos previstos en el propio reglamento (RGPD), a oponerse a que la empresa realice un tratamiento de sus datos personales y que este deberá de no tenerlos en cuenta en cuanto a su tratamiento. Estos casos son:

- Si los datos se tratan lícitamente en cuanto a el cumplimiento de una misión que puede ser de interés público, desarrollo de poderes públicos y finalmente intereses legítimos.

- Los datos personales del usuario se van a usar, o van a ser tratados con fines de mercadotecnia directa (elaboración de perfiles).

Este derecho ya estaba recogido en el LOPD, por lo que no se trata de una novedad por parte del RGPD, sin embargo, hay que distinguir entre retirar el consentimiento al tratamiento de los datos, que hemos visto anteriormente, con el derecho de oposición.
Uno de los aspectos más interesantes es cuando tiene fines de mercadotecnia. La mercadotecnia es una forma de comunicación digital de manera que se usa los datos de cada uno de los individuos para enviarle a través distintos canales (redes sociales, emails, spam, anuncios en la web, etc.) publicidad.
No existe ningún tipo de excepción a este caso, por lo que el responsable no podrá usar los datos con fines de mercadotecnia directa, incluyendo en este tratamiento la elaboración de perfiles.
Este derecho tiene una gran importancia en el sentido que evita el tratamiento de datos con fines que sean ajenos al fin de su recopilación. El hecho de que se tenga en cuenta la mercadotecnia es un indicio del tipo de traspasos de datos que existen hoy en día. Un ejemplo de ello es la correlación que hay cuando realizamos una búsqueda a través de un motor de búsqueda, y la publicidad que empieza a salir en distintos canales.
El hecho que existe la posibilidad de evitar este tipo de actuaciones demuestra el avance que han aportado la regulación con el fin de proteger la toma de decisiones y por ende la capacidad de control de los usuarios de que se hace con sus respectivos datos personales.
Se trata en cierta manera de evitar una intromisión en la vida privada de cada uno de los usuarios cuando ejercitan este tipo de derecho. El hecho de evitar que se realice el tratamiento de datos con un objetivo de mercadotecnia directa evita que se entrometan y usen datos personales para lanzar publicidad que para este pueda ser molesto, o que simplemente no le interese recibir al usuario.
Se trata también de un efecto que tiene el principio de consentimiento y que da la opción a ejercitar un derecho que impide el tratamiento de datos.

7 LA EXCLUSIÓN ÉTICA EN LA REGULACIÓN DE LA PROTECCION DE DATOS

Las regulaciones tanto públicas como el RGPD a nivel europeo y la LOPD a nivel estatal, como las privadas como la *California Consumer Privacy Act* (CCPA), están en ambos casos diseñados para proteger al consumidor en todo momento. Los principios y derechos más importantes del RGPD y LOPD, son muestra de la protección a los usuarios o que se busca con la regulación de dichos reglamentos o directivas.

Sin embargo, el RGPD, al igual que el CCPA, no regula el procesamiento de datos en si, por lo que todavía existe una parte de la protección de datos que no está clara. Eso es debido al gran avance en las tecnologías que se han desarrollado a lo largo de los últimos 5 años. El proceso que se realiza de los datos y el tratamiento de estos ha evolucionado mediante aprendizaje automáticos y mediante la Inteligencia Artificial (IA). Estos procesos que realizan estas tecnologías no tienen constancia en la regulación tanto europea como nacional. Es decir, no contemplan la regulación ética que las empresas deben realizar a la hora de usar los datos de sus clientes[35]. De esta forma existe un impacto negativo sobre los usuarios en cuanto al resultado y al uso que realizan de sus datos.

El control que nos ofrece la regulación, tanto el RGPD como el LOPD, no es suficiente para paliar los daños que pueden realizar los algoritmos que se usan en los distintos tipos de tratamiento de datos.

"¿Es el GDPR suficiente? Parece obvio que no. Los datos son la materia prima de la era de la información y su comercio es muy lucrativo. Estos datos alimentan las inteligencias artificiales que determinan en buena medida qué hacemos, qué compramos o a dónde vamos de vacaciones. Está claro que dejar el control de los algoritmos a las empresas que los crean es como dejar al zorro vigilando a las gallinas."[36]

[35] Floridi, L. and Taddeo, M. (2016). What is data ethics?. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 374(2083), p.0360.

[36] Orbe, A. (2018, 12 diciembre). *Ética y Big Data*. Telos Fundación Teléfonica. (Disponible en: https://telos.fundaciontelefonica.com/etica-y-big-data/; última consulta 01/04/2021)

Uno de los principales problemas radica en el autoaprendizaje de los algoritmos ya que estos están diseñados para que su eficiencia aumente al igual que su utilidad y eficacia, y aprenden por ellos mismo. En cierta manera, la IA presenta la posibilidad de realizar sesgos de realidades con las que la mentalidad humana no está acostumbrada. Se pueden obtener casos de predicciones y clasificaciones en base a perfiles de datos que no estan conformes a la realidad.

El control que brinda las distintas regulaciones, tanto europeas como nacionales, siguen sin ser conformes a la realidad de manera que no se ajustan a los fines reales del tratamiento de datos.

Todos los principios y derecho que regula no tienen ninguna utilidad, si el proceso o el tratamiento de los datos de los usuarios son en cierta manera tratados de una forma distinta a la que los usuarios piensan, y de los cuales se obtienen resultados distintos.

Para ello, se examinan distintas soluciones y aparece lo que se conoce hoy en día como el "*Data Ethics*". Se trata de un programa mediante el cual el consumidor conocerá y tendrá más información con respecto a cómo se utilizan, cómo se procesan y cómo se comparten sus datos de manera a paliar el impacto negativo de que supone compartir información personal.

"Data Ethics se ocupa principalmente de la propiedad, la transparencia, el consentimiento, la privacidad, su valor financiero y su disponibilidad. Además, para implementar este programa regulatorio, BDO establece un Marco sobre la gestión ética de los datos basado en cuatro puntos clave:

1. *Definir claramente el proyecto y los objetivos para establecer de manera clara los problemas que se quieren resolver y a quienes va a beneficiar. El resultado debe mostrar los riesgos potenciales o las consecuencias negativas de continuar con el proyecto.*
2. *Desarrollar un programa transparente a través del cual la compañía se responsabilice del uso de datos. La transparencia en el uso de los datos y la responsabilidad de protegerlos, fomentan una transición clara a la creación de un Marco sobre la gestión ética de los datos, proporcionando a los consumidores el conocimiento de los datos que se recopilan sobre ellos, cómo se utilizarán y permitiendo que estos soliciten la eliminación de aquella información que no quieran compartir.*
3. *Usar los datos de forma proporcional al proyecto. Las empresas deben emplear la cantidad mínima de datos relevantes necesarios para lograr resultados*

específicos. Además, se debe evaluar si la información recopilada es necesaria, o, por el contrario, se puede prescindir de ella.

4. *Por último, se deben comprender las limitaciones de los datos para mantener su integridad y considerar si serán necesarias salvedades para futuras políticas o procedimientos."*
5. *Sin embargo, el impacto que tiene el programa de "Data Ethics" es mínimo ya que se tratan de procesos propios de la empresa y no tiene ninguna vinculación como tal en la regulación. De nuevo existe por ello una desconfianza generalizada ante el tratamiento de datos, ya que no existe un respaldo legislativo."* [37]

8 FUTURO INCIERTO

Hoy en día, sigue existiendo un problema en cuanto al futuro de la regulación de la protección de datos con respecto al avance tecnológico del tratamiento de la información. El avance es cada vez más rápido y no da tiempo a que las regulaciones de todos los aspectos relevantes se realicen en tiempo y en forma, dando lugar así, a situaciones desconocidas y en las cuales no existe una protección jurídica para los usuarios y sus datos.

Por ello, se podría, según Rosa Colmenarejo Fernández, establecerse dos tipos de corrientes en cuanto al futuro de la regulación del *Big Data* y de las nuevas tecnologías[38]. Por un lado, se encuentra una corriente que busca aguantar con la regulación existente, y que conforme las tecnologías del tratamiento de datos vayan avanzando, se incorpora regulaciones al respecto. Es decir, este tipo de pensamiento busca en un primer momento, no anticiparse a las posibles consecuencias de un mal uso del *Big Data*. Hoy en día, parece que esta corriente es la principal, en el sentido que la regulación parece estar esperando a que avancen las tecnologías de tratamiento de datos, para después ponerles freno mediante regulaciones.

[37] J Orbe, A. (2018, 12 diciembre). *Ética y Big Data*. Telos Fundación Teléfonica. (Disponible en: https://telos.fundaciontelefonica.com/etica-y-big-data/; última consulta 01/04/2021)

[38] Colmenarejo Fernández, R. (2017), "Ética Aplicada a la Gestión de Datos Masivos"

Dentro de esta corriente, a su vez, distinguimos dos tipos, una primera mas precavida en la que se busca en cierta manera seguir controlando la protección de datos incorporando ciertas regulaciones a lo largo del tiempo, y otro tipo mucho mas permisiva. En esta última, existe una confianza en la buena fe de las empresas y en el tratamiento de datos. Se podría comparar, en cierta manera, con el concepto de "*laissez faire*", de manera que la cuestión ética vinculada a la protección de datos no tenga una relevancia tan importante en el momento, y que así, no frene el avance tecnológico que puede ser beneficioso para muchos sectores. Una vez que los avances se hayan realizado se entrará a regular dichos avances.

Lógicamente, este pensamiento resulta perjudicial para los derechos de los usuarios, y se basa en el buen uso de los datos de sus usuarios por las empresas. Los casos como el de "*Cambridge Analytics*" en 2015, y el colosal caso de "*Google*" en 2018, son pruebas más que suficientes para que esta corriente no sea la correcta.

No obstante, el otro tipo de corriente en cuanto al futuro ético de la protección de datos y su regulación con respecto del *Big Data* parece tener un cierto un aspecto mucho más precavido. En el sentido que esta corriente, aboga por adelantarse al avance tecnológico y en cierta manera regular el futuro de este. A su vez, no está claro, ya que ¿cómo vas a regular aspectos jurídicos y procesos que todavía no existen? Parece algo que de momento es difícil de realizar. Por ello, una solución a este pensamiento es regular de manera a que exista un mayor control sobre los procesos de tratamiento de datos, y sobre todo conceder a los usuarios mayor control sobre sus datos y blindar los derechos como el consentimiento y como el derecho de olvido.

9 CONCLUSIONES

El objetivo del trabajo se basa analizar la regulación que existe hoy en día con respecto a la protección de datos y analizar los distintos derechos y mecanismos de control que tiene, y su relación con la moral o la ética de este frente a las nuevas tecnologías como el *Big Data*.

La regulación de la protección de datos ha ido tomando cada vez más y más relevancia a lo largo de los últimos años debido al enorme avance de las tecnologías relacionadas con el tratamiento de datos o *Big Data.* El RGPD de 2018, ha aportado una serie de novedades

en cuanto a mecanismos de control y derechos, dejando atrás otras normativas al respecto. En un principio, el RGPD se pretende proteger siempre los intereses de los usuarios y el tratamiento de datos que las empresas puedan realizar, otorgando una serie de mecanismos de control en cuando a las empresas y una serie de acciones con respecto de los usuarios. Además, aporta un régimen sancionador para aquellos casos en los que hubiera una vulneración de los derechos que se buscan defender.

El RGPD contribuye con mecanismos de control y son una muestra del avance que supone para la defensa de la privacidad en cuanto a la protección de datos. Las políticas de protección de datos, los Códigos de Conducta, los mecanismos de certificación, etc aportan un gran avance en cuanto al control de las empresas y al tratamiento que hacen de los datos. Este control, además esta supervisado por una figura de **autoridad**, la cual se encarga de comprobar y acreditar, que el uso que se hace de los datos personales de los usuarios está de acuerdo con el reglamento, dando lugar a infracciones en caso de que no sea así. Sin embargo, salvo para la minimización de datos, todas son optativas o voluntarias, por lo que realmente **no tienen un carácter obligatorio**. Esto genera en cierta manera una **inseguridad**, ya que no todas las empresas cumplirán y, por ende, no darán una garantía de que cumplen con los mecanismos de control figurados en el RGPD. Esta inseguridad da lugar a una desconfianza por parte de los usuarios a que las empresas están haciendo un uso correcto de sus datos y que de cierta manera cumplan y respeten la privacidad de los usuarios.

No obstante, la regulación del RGPD, presenta una serie de derechos por parte de los usuarios, para que de cierta manera aquellos que den sus datos tengan siempre la última palabra. Todos estos principios nacen y se basan en el principio del **consentimiento**, en donde media la voluntad propia, o la autonomía de voluntad. A diferencia de los mecanismos de control, los derechos que se regulan en el RGPD tienen un **carácter coercitivo** para las empresas, y brindan la oportunidad al usuario o al individuo que cede sus datos a las empresas a conocer que se van a hacer con ellos, y con que finalidad se recogen. Sin embargo, la información que se les da a los usuarios para ceder esos datos muchas veces es vaga, y todavía el usuario común no es consciente de lo que esta haciendo al ceder sus datos o al permitir a la empresa el uso de sus datos. De la misma manera, existen otros derechos como el **derecho al olvido** o el **derecho a la portabilidad**, que otorgan al usuario o al individuo un control cada vez mayor sobre los datos, incluso

cuando ya los ha cedido. Por ello, los avances que ha aportado el RGPD, son de gran utilidad para el usuario y brinda una gama de posibilidades en cuanto al control por su parte de sus propios datos, al igual que recibir la información que necesita. Sin embargo, todavía se necesita desarrollar muchos de estos derechos y otorgarlos mas poder de control, al igual que dar la posibilidad a los usuarios de obtener más información relevante y precisa con respecto al fin de su recopilación.

El futuro de la regulación de la protección de datos es bastante impreciso, ya que el avance de las tecnologías sobrepasa en gran medida el avance de la regulación al respecto. La posibilidad de regular hoy en día muchos aspectos que aún no se han comprobado o que no han dado lugar a problemas parece algo imposible.
De la misma manera, tener una actitud pasiva frente al avance de las tecnologías provocará infracciones en un futuro, al igual que quebrantamientos de derechos fundamentales como es el derecho a la privacidad

10 BIBLIOGRAFÍA

10.1 Legislación

-Carta de los Derechos Fundamentales de la Unión Europea, Diario Oficial Nº. C. 303, de 14/12/2007.

-Constitución Española de 1978. «BOE» núm. 311, de 29/12/1978, Referencia BOE-1978-31229.

-Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal

-Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, *Boletín Oficial del Estado* no 294, de 6 de diciembre de 2018.

-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*). *Diario Oficial de la Unión Europea,* L 119/1, de 4 de mayo de 2016.

10.2 Obras Doctrinales

- Aleecia, M. M., & Cranor, L. F. (2008). The cost of reading privacy policies. *Information System: A journal of law and policy for the information society. Available at www. is-journal. org*.

- Auñón, N. R. (2019). Los códigos de conducta y las certificaciones en el RGPD (Arts. 40-43 RGPD. Arts. 38-39 y Disposición transitoria segunda LOPDGDD). In *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD* (pp. 549-568). Wolters Kluwer.

- Bennett, C. J. (1992). *Regulating privacy: Data protection and public policy in Europe and the United States*. Cornell University Press.

- Berinato, S. (2014). With big data comes big responsibility. *Harvard Business Review*, *92*(11), 20.

- Garriga Domínguez, A. (2016). *Nuevos retos para la protección de datos personales. En la Era del Big Data y de la computación ubicua*. Dykinson.

- Gil, E. (2016). Big data, privacidad y protección de datos. *Madrid: Agencia Estatal Boletín Oficial del Estado*.

- Goldsteen, A., Ezov, G., Shmelkin, R., Moffie, M., & Farkash, A. (2020). Data Minimization for GDPR Compliance in Machine Learning Models. *arXiv preprint arXiv:2008.04113*.

-Heuer, H., & Breiter, A. (2018). Student success prediction and the trade-off between big data and data minimization. *DeLFI 2018-Die 16. E-Learning Fachtagung Informatik*.

- Lachaud, E. (2018). The General Data Protection Regulation and the rise of certification as a regulatory instrument. *Computer Law & Security Review*, *34*(2), 244-256.

-Floridi, L. and Taddeo, M. (2016). What is data ethics?. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, p.374.

- Frisk, J. E., & Bannister, F. (2017). Improving the use of analytics and big data by changing the decision-making culture. *Management Decision*.

- Marr, B. (2016). *Big data in practice: how 45 successful companies used big data analytics to deliver extraordinary results*. John Wiley & Sons.

- Vázquez, F. M. (2019). El reciente marco de la protección de datos personales (RGPD y nueva LOPDP): las obligaciones del responsable y del encargado, el Delegado de

Protección de Datos y el régimen sancionador. *Rued@. Revista Universidad, Ética y Derechos*, 41-57.

- Ortigosa, A. P. (2019). Decisiones automatizadas en el RGPD. El uso de algoritmos en el contexto de la protección de datos. *Revista general de Derecho administrativo*, (50).

- Rallo Lombarte, A. (2019). El nuevo derecho de protección de datos.

-Ramiro, M. A. (2005). El derecho fundamental a la protección de datos personales en Europa (Doctoral dissertation, Universidad de Alcalá).

- Shaqiri, Bledi. (2017). Exploring Techniques of Improving Security and Privacy in Big Data. 10.13140/RG.2.2.23201.10089.

- Schneble, C. O., Elger, B. S., & Shaw, D. (2018). The Cambridge Analytica affair and Internet-mediated research. *EMBO reports*, *19*(8), e46579.

- Zarsky, T. Z. (2016). Incompatible: the GDPR in the age of big data. *Seton Hall L. Rev.*, *47*, 995.

10.3 Recursos de Internet

- Big Data: ¿En qué consiste? Su importancia, desafíos y gobernabilidad. (Disponible en: https://www.powerdata.es/big-data; última consulta 12/03/2021)

-Derecho a la privacidad en España. (Disponible en: https://ayudaleyprotecciondatos.es/2018/11/13/derecho-privacidad-espana/#:~:text=El%20art%C3%ADculo%2018%20de%20la,intimidad%20y%20a%20la%20imagen%20personal.&text=El%20RGPD%20o%20Reglamento%20Europeo,en%20todo%20el%20territorio%20europeo; última consulta 14/03/2021)

- Francesc, JM. (2019,27 febrero) Ética, anonimización y Big Data. (Disponible en: https://cincodias.elpais.com/cincodias/2019/02/27/legal/1551257290_537953.html; última consulta 01/04/2021)

-González, Y. (2021, 17 marzo). *Derecho al Olvido en el RGPD*. Grupo Atico34. (Disponible en: https://protecciondatos-lopd.com/empresas/derecho-olvido-rgpd/; última consulta 01/04/2021)

- Orbe, A. (2018, 12 diciembre). *Ética y Big Data*. Telos Fundación Teléfonica. (Disponible en: https://telos.fundaciontelefonica.com/etica-y-big-data/; última consulta 01/04/2021)

- Ortiz, P. (2018, 24 diciembre). La protección de datos, un asunto profundamente humano". Universidad Europea (Disponible en: https://www.elcomercio.es/sociedad/proteccion-datos-asunto-20181224165559-nt.html?ref=https:%2F%2Fwww.google.com; última consulta 01/04/2021)

- Serrano A. Big Data y protección de datos. (Disponible en https://www.antonioserranoacitores.com/big-data-proteccion-datos/#312_Recursos_responsabilidad_y_sanciones; última consulta 15/03/2021)

- Tablado F. Ley de Protección de Datos y Garantía de Derechos Digitales (LOPDGDD) 2018. (Disponible en: https://protecciondatos-lopd.com/empresas/nueva-ley-proteccion-datos-2018/; última consulta 15/02/2021)