**Universidad Internacional de La Rioja**

**Máster en Protección de Datos**

# [La protección de datos en entornos de Big Data]

Trabajo fin de máster presentado por: Carlos Rosales González

Titulación: Máster Universitario en Protección de datos.

Área jurídica: Tecnologías emergentes y Protección de Datos.

Director/a: Javier Puyol Montero.

Santander

20/03/2019

Firmado por: Carlos Rosales González

# Índice

# I. Listado Abreviaturas

AEPD - Agencia Española Protección de Datos.

ARCO - Derechos Acceso, Rectificación, Cancelación y Oposición.

Art - Artículo.

CdE - Consejo de Europa.

CE - Constitución Española.

CE – Comisión Europea.

EEE - Espacio Económico Europeo.

EIPD - Evaluación de Impacto en Protección de Datos.

EU RD PLATFORM - *European Platform on Rare Disease Registration*

GT29 - Grupo de trabajo del artículo 29.

Hash - Función Hash.

LOPD - Ley Orgánica de Protección de Datos 15/1999.

LOPDGDD - Ley Orgánica de Protección de Datos Y Garantía de los Derechos Digitales 3/2018.

LSSI - Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico

ORION - *On-Road Integrated Optimization & Navigation.*

OYSTER - *Oyster smartcard ticketing system*.

PPE - Parlamento Europeo.

PYME – Pequeña y Mediana empresa.

RGPD - Reglamento Europeo de Protección de Datos.

RLOPD - Reglamento de desarrollo de la Ley Orgánica de Protección de Datos.

RFID - *Radio Frequency Identification*.

UE - Unión europea.

# II. Resumen/Abstract.

**Resumen**

Este trabajo intenta explicar en qué consiste el Big Data, como diferenciar esta tecnología y dar a conocer algunos casos de éxito de esta, con la finalidad de comprender su importancia y afrontar la problemática existente entre su utilidad y su encuadramiento en la nueva regulación de protección de datos.

También se analiza como las empresas utilizan el Big Data dentro de la protección de datos, con que bases legitimadoras, y la situación de la anonimización como salida al conflicto existente.

**Palabras Clave:** BIG DATA, PROTECCIÓN DE DATOS, ANONIMIZACIÓN.

**Abstract**

This paper tries to explain what Big Data consists of how to differentiate this technology and present some success stories, in order to understand its importance and face the existing problem between its usefulness and its framework in the new protection regulation of data.

It also analyzes how companies use Big Data within data protection, with which legitimizing bases, and the situation of anonymization as an exit to the existing conflict.

**Keywords**: BIG DATA, DATA PROTECTION, ANONYMIZATION.

# III. Introducción

La elección de este tema para la realización del trabajo final de Máster no es casualidad. La protección de datos es un tema de actualidad absoluta y el Big Data es una tecnología emergente y de utilidad con numerosos beneficios para la sociedad. La contradicción entre la privacidad y el tratamiento masivo de datos es un tema interesante para tratar en este trabajo final de máster.

La privacidad de los individuos se ha visto alterada en los últimos años por el surgimiento de las tecnologías de la información y principalmente internet, la nueva normativa intenta paliar este déficit que ha existido en estos últimos años entre una normativa antigua y desfasada frente a una tecnología que avanza cada año de maneras diversas, ahora este déficit se ha intentado paliar con una normativa homogénea a nivel europeo en forma de reglamento.

En este trabajo se intenta explicar que es el Big Data y como puede encuadrarse dentro de la normativa europea y española, desentrañando las peculiaridades, los pros y las contras respecto a la protección de datos personales.

La búsqueda de este encuadramiento en la normativa de esta nueva tecnología es el fin de este trabajo, considerando el Big Data como una oportunidad beneficiosa para la sociedad, pero con situaciones mejorables para la privacidad de los usuarios, como es el consentimiento expreso para la anonimización de datos personales y la utilización de estos con fines estadísticos y de mejora.

# IV. Big Data.

El Big Data es una palabra anglosajona, este término es acuñado por primera vez por John Mashey en el año 1998. Fue usado por este científico informático, en un artículo publicado en el New York Times: "*Big Data and the Next Wave of Infrastress*".

El mismo autor comentó al respecto posteriormente, que su intención era utilizar una terminación sencilla que abarcara el creciente alcance de los sistemas de computación. Este nuevo término es hoy en día muy usado, comprende desde datos generados por sistemas tradicionales hasta nuevas formas digitales de comunicación y de información compartida. En castellano podríamos traducirlo como "*Datos Masivos"*[1], en este término podríamos aglutinar, el conjunto de tecnologías, o procesos empleados para captar datos a un nivel y diferenciación no alcanzada previamente, y conseguir extraer valor de esta información, gracias a la posibilidad que nos dan los sistemas analíticos avanzados soportados por computación.

En el mundo informático, los Datos Masivos (en adelante Big Data), son tendencia de alta complejidad, esto es debido a que la mayoría de los datos originados no son estructurados, por ejemplo:

- Redes Sociales: Instagram, Facebook, Twitter, LinkedIn…
- Smartphones, Tablets...
- Dispositivos GPS.
- Búsquedas en navegadores de internet.
- Registros de centros de llamadas…

Estos datos sin estructurar no entrañan ningún valor añadido por si solos, el Big Data se basa en la tecnología para poder extraer valor, los equipos informáticos tradicionales no son capaces de procesar un volumen tan denso de datos, por esa misma razón, nació el denominado Big

[1] MANDADO PÉREZ-FERNÁNDEZ SILVA-MARCOS ACEVEDO-ARMESTO QUIROGA-RIVAS LÓPEZ-NÚKEZ ORTUÑO (2018:11)

Data, con un conjunto de herramientas informáticas se es capaz de almacenar, y tratar dicha información.

La era de la información cambio el mundo, la llegada de internet fue una revolución a nivel mundial, y la llegada del Big Data está cambiando de nuevo la percepción de muchas cosas, la eficiencia o valor añadido que se puede obtener de determinados datos es inimaginable.

La idea es en sí misma sencilla: extraer a raíz de tratar volúmenes gigantescos de información, utilidades y beneficios antes inimaginables con pequeñas bases de datos, las consecuencias del uso del Big Data solo las descubrirá el futuro, ya que las posibilidades son amplias, por no decir infinitas. Por ahora podemos ver su influencia en determinados campos, pero su diversificación y futuro es prometedor.

Antiguamente, los valores obtenidos no tenían ningún valor añadido, podríamos definirlos como datos estáticos, de un solo uso, o diversos usos muy específicos, con el devenir de las nuevas tecnologías, el tratamiento de estos datos (inútiles a simple vista para más de un uso) ha derivado en una obtención de riqueza y conocimiento sin igual. Cuando queremos hacer una búsqueda en un navegador de internet, no valoramos que nuestro acto incida más allá de una mera búsqueda en el navegador, pero en realidad estamos dándole a la multinacional dueña del navegador datos importantes, que pueden convertirse con un estudio adecuado, en un valor añadido para la empresa, para un país o incluso para la sociedad.

La correlación de búsquedas en navegadores web, puede detectar midiendo palabras clave, la preocupación de determinadas zonas de población por determinadas enfermedades, ataques terroristas, por los niveles de paro de la región...

Estos datos de búsquedas pueden ser correlacionados por ejemplo con los datos de salud del gobierno en una colaboración y determinar con un alto grado de coincidencia, que cuanta más gente está enferma por constipado, más búsquedas como “remedios” para el “constipado” habrá por poner un ejemplo. El Big Data ha llegado para revolucionar el mundo en el que vivimos. Pero el tratamiento de datos tal y como se conoce esta intrínseco en nuestro día a día, somos plenamente conscientes de que las nuevas tecnologías han llegado para quedarse y nos facilitan el desempeño de nuestras actividades cotidianas, tanto en el trabajo como en la vida personal.

Diferenciar un análisis de datos normal y corriente a un tratamiento de Big Data, implica especificar que es el Big Data, cómo cuantificamos qué es y qué no es.

# V. ¿Cómo identificar el Big Data?

Para comprender que es este fenómeno del Big Data y su dimensión, debemos empezar por conocer las denominadas "cinco V".

## V.1. Las Cinco V del Big Data.

Al Big Data se le desentraña gracias a estas diferentes fases o etapas, algunos autores difieren de la cantidad de "V" que pueden definirlo, ampliando el abanico a siete y otros disminuyéndolo a tres, pero en definitiva estas son las más representativas.

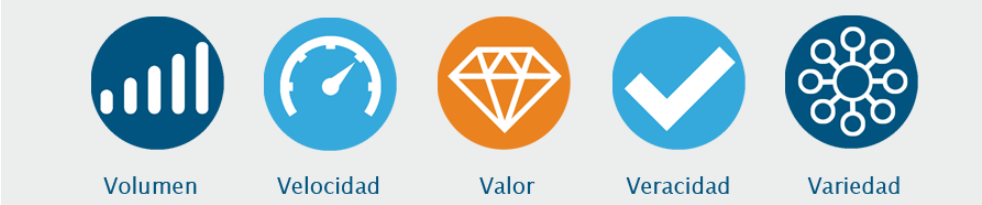


*Tabla 1. Cinco V del Big Data*[2]

- La primera "V" que especifica el rango del Big data es el denominado volumen. Usaré la definición de la Agencia Española de Protección de Datos (en adelante AEPD), en su guía de buenas prácticas en proyectos de Big Data: **Volumen**[3] "*es la característica más obvia y que recoge el propio nombre de Big Data. Se pasa de manejar magnitudes de megabytes, gigabytes, como mucho Terabytes, a manejar Petabytes (1.000.000.000.000.000 Bytes) de forma cada vez más frecuente. Este volumen de datos es tan grande que ya no puede ser analizado mediante herramientas y procesos tradicionales tales como MS Excel o SQL. Ha sido necesario comenzar a utilizar nuevos sistemas, como NoSQL o el software Apache Hadoop.*" La

[2] Tabla: Cinco V del Big Data. Quental. Disponible en: https://www.quental.com/services/big-data.html. Referencia: 17 de marzo 2019.

[3] ACED-HERAS-SÁIZ (2018: 8).

evolución tecnológica, varía lo que consideramos Big Data, ya que cada vez nos permite tratar volúmenes de datos más grandes con menos dificultad. La idea para tener en cuenta es que, para enmarcar el Big Data según el volumen, hablamos de cantidades ingentes de datos. El tratamiento de datos en una oficina de una PyME, no es un tratamiento de datos en un entorno Big Data, se necesitan cantidades masivas solo abarcables por programas especiales o servidores preparados para tal ardua tarea.

- Otra variable diferenciadora es la **Variedad**, la cual se enmarca en la naturaleza de los datos, las diferentes fuentes de donde proceden, cuantas más de estas fuentes tengamos, siempre que podamos relacionar estos datos, implicara tener una base de datos superior, o más completa. Los datos pueden proceder de diferentes sitios, ya sean redes sociales, dispositivos de tecnología de Radio frecuencia (*Radio Frequency Identification*, en adelante RFID), encuestas, smartphones... Todos ellos permiten conocer hábitos de vida, dispositivos electrónicos conectados a la red, e-mails, smartphones, páginas web, blogs etc. La principal innovación es tratar datos de diferentes fuentes, estructuradas, semi estructuradas o desestructuradas, es decir datos dinámicos en continuo cambio a como era previamente (datos estáticos y de fuentes internas).

- Otro factor distintivo es la **Velocidad**, esta hace referencia a un elemento de vital importancia, el tiempo. Con las tecnologías adecuadas, la recepción, transferencia y procesado de datos se hace a una velocidad cada vez mayor, incluso a tiempo real. Analizar datos en tiempo real, puede ser una ventaja, incluso competitiva en el mundo empresarial, para darnos ventajas tales como en la detección de errores, fraude o realización de ofertas especificas adelantándose a competidores.

- No menos importante es el concepto de **Veracidad** de los datos, este hace referencia directa a la calidad de los datos, la calidad es de vital importancia, si un dato no está estructurado, puede crear incertidumbre sobre su fiabilidad, por ello, la captura de datos de diversas fuentes puede ayudar a minimizar la incertidumbre, al igual que la verificación, o limpieza, para sacar el mayor provecho de estos, y ser lo más fiables posibles.

- Por último, encontramos la razón de ser del Big Data, el **Valor**, la finalidad final de hacer un tratamiento de datos masivos es obtener un valor añadido que reporte conocimiento.

Estas cinco V, conforman lo que consideraríamos Big Data, un almacenamiento y una estructura de los datos capaz, una rápida velocidad de captura, procesamiento y análisis, una confiable calidad de los datos, a su vez que variedad en los mismos, todo ello orientado a confiar en su fiabilidad y minimizar la incertidumbre, llevaran a una empresa, ente público, organización, fundación, persona física, etc. A obtener valor añadido haciendo uso del concepto Big Data.

# VI. Protección de Datos en el entorno del Big Data

A pesar de todos los beneficios prometedores que pueda tener el Big Data, también hay razones para ser precavido, sí antes del Big Data, para intentar discernir posibilidades futuras existían métodos de predicción a través de muestras representativas y el resultado era orientativo, actualmente podemos tratar todos los datos sin necesidad de muestras y automáticamente conocer todos los resultados de manera inequívoca, esto es un riesgo para nuestra privacidad, y para nuestra libertad. Ya que, al cruzar bases de datos, se pueden identificar datos personales y conocer determinados factores utilizando la correlación. En definitiva, se ha alcanzado un nivel de tratamiento tan grande que no son necesarias las muestras representativas, se puede conocer con exactitud todos los datos de un determinado estudio, aunque sea masivo.

La evolución tecnológica permite analizar todos los datos de una manera muy sencilla, por tanto, las bases de datos han crecido y se nutren de información de diferentes fuentes que logran formar bases de datos completas y fácilmente relacionables con otras bases de datos o datos públicos.

La protección de datos es un derecho fundamental reconocido en el artículo 8.1 de la carta de los Derechos Fundamentales de la UE, y en el artículo 16.1 del Tratado de Funcionamiento de la UE, donde se establece que toda persona tiene el derecho a la protección de datos personales.

En España, este derecho fundamental está recogido en nuestra Constitución[4], donde se hace mención del derecho al honor, a la intimidad personal y familiar y a la propia imagen. También nos especifica que "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".[5]

Aquí es donde entra la Protección de Datos. Este concepto engloba la legislación vigente en materia de datos para proteger al ciudadano del uso de sus datos personales con finalidades para los que no fueron recabados o regular un cierto nivel de seguridad y protección jurídica para los mismos. Dependiendo del lugar en el que nos encontremos, la legislación será más o menos estricta. En nuestro caso, nos encontramos en la Unión Europea, donde está vigente el RGPD. Y en concreto en España, donde está vigente la nueva LOPDGDD, esto implica que tenemos nueva legislación respecto a la antigua Directiva, Ley Orgánica de Protección de Datos y Reglamento de Desarrollo, que implica algunos cambios que veremos posteriormente.

**¿Qué es un Dato Personal y que implica?**

La definición de un dato personal la tenemos en el artículo 4 del RGPD:

*"«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 propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;"*[6]

[4] Artículo 18.1, CE. Boletín Oficial del Estado. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-1978-31229 Referencia: 17 de noviembre de 2018.

[5] Ídem, Artículo 18.4

[6] Artículo 4, RGPD. Boletín Oficial del Estado. Disponible en: https://www.boe.es/doue/2016/119/L00001-00088.pdf Referencia: 18 de noviembre de 2018.

Se entiende que un gran número de los datos utilizados en Big Data pueden ser datos de carácter personal, entrando de esta forma dentro de la legislación vigente y por tanto en la obligación de cumplir una serie de reglas. La implicación de estas es lo que se tratará de explicar a continuación. Igualmente se debe comprender que todo dato que no identifique a una persona no será un dato personal y no deberá cumplir con las leyes de protección de datos, lo cual puede ser la clave para el caso del Big Data.

En este 2018, la sociedad se encuentra en un año de cambio a nivel normativo respecto a los datos personales, el nuevo Reglamento General de Protección de Datos, es de aplicación desde el 25 de mayo de 2018, la nueva Ley Orgánica de Protección de Datos que deroga la antigua de 1999, también entro en vigor a finales de año. Lo cual cambia las reglas y las moderniza, hay que tener en cuenta que la evolución tecnológica ha sufrido un boom en las últimas décadas, pero la legislación no ha evolucionado al mismo ritmo, por tanto, el nuevo reglamento europeo y las leyes nacionales que lo desarrollan. Nacen de esta necesidad.

Como indica el RGPD en sus considerandos número 6 y 7. Donde nos expone que, ante la magnitud de los tratamientos que se realizan en nuestros días, y las novedades tecnológicas emergentes, se necesita una normativa acorde para hacerle frente a las nuevas problemáticas existentes.

Dentro de esta normativa existen varios tipos de bases legitimadoras para el tratamiento de datos personales en entornos de Big Data y también como convertir los datos personales en datos anonimizados. Entendiendo que el tratamiento de datos en el ámbito del Big Data muchas veces chocara de lleno con la normativa creando cierta controversia entre la búsqueda de privacidad y una tecnología “opuesta “a priori a este derecho constitucional.

Cabe resaltar que la nueva normativa europea, abarca todo tratamiento de datos correspondiente a un responsable o encargado del tratamiento dentro del Espacio Económico Europeo (en adelante EEE) independientemente de si los datos son de este espacio o no, e incluso ha ampliado su ámbito a aquellos responsables no establecidos en este espacio económico europeo, en los casos en los que el tratamiento de datos personales esté relacionado con oferta de bienes

o servicios destinados a ciudadanos europeos o como consecuencia de monitorización del comportamiento dentro de la UE, lo que conlleva a un ámbito mundial de la normativa.

# VII. Bases Legitimadoras en entornos de Big Data.

Basándonos en el RGPD, hay varias bases legitimadoras para realizar un tratamiento de datos personales, pero existe la obligación de cumplir al menos una de ellas, sea el consentimiento u otra base legitima[7].

En entornos del Big Data analizaremos varias bases legitimadoras principales para el posible tratamiento de datos.

## VII.1. El Consentimiento.

El consentimiento expreso, constituye la mayor novedad en el nuevo reglamento, y la nueva LOPDGDD recién aprobada[8], en el senado. Se ha visto actualizada la normativa a los nuevos tiempos modernos, y los requisitos relacionados con el consentimiento también han sido renovados, ya no basta con un consentimiento tácito, como vamos a ver, la legislación se ha vuelto más proteccionista.

El consentimiento ha variado sustancialmente desde la aplicación del nuevo RGPD

Podemos comenzar contestando a la pregunta, ¿Qué es el consentimiento del interesado?, para ello utilizaremos la definición de consentimiento que viene dada en el artículo 4.11 del RGPD:

[7] Ídem. Considerando 40.

[8] LOPDGDD. Boletín Oficial del Estado. Disponible en: https://boe.es/boe/dias/2018/12/06/pdfs/BOE-A-2018-16673.pdf Referencia: 15 de enero de 2019.

*"«consentimiento del interesado»: 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."*[9]

Para comprender los cambios y las obligaciones en la obtención del consentimiento, vamos a analizar la nueva reglamentación, partimos de la base del considerando número 32 del RGPD,

"*El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca …"*[10]

Este consentimiento debe ser claro, libre, especifico, informado e inequívoco. Y el punto importante, que este consentimiento debe ser específico para cada tratamiento de datos, teniendo en cuenta la magnitud de los tratamientos del Big Data y la correlación de datos personales, es virtualmente posible pensar que la utilización de esta nueva tecnología llevara intrínseco el riesgo inherente de hacer nuevos tratamientos sin el consentimiento oportuno del interesado ante la dificultad más que manifiesta de recabar el consentimiento de una cantidad importante de personas.

Este considerando no es el único referente al consentimiento, tenemos que tener en cuenta más considerandos del RGPD que dan forma al consentimiento de cara a obtenerlo, tales como:

Considerando número 42:

*"Cuando el tratamiento se lleva a cabo con el consentimiento del interesado, el responsable del tratamiento debe ser capaz de demostrar que aquel ha dado su consentimiento a la operación de tratamiento..."*[11]

[9] Artículo 4.11, RGPD. Boletín Oficial del Estado. Disponible en: https://www.boe.es/doue/2016/119/L00001-00088.pdf Referencia: 12 de febrero de 2019.

[10] Ídem. Considerando 32.

[11] Ídem. Considerando 42.

Y considerando 43:

"….. *Se presume que el consentimiento no se ha dado libremente cuando no permita autorizar por separado las distintas operaciones de tratamiento de datos personales pese a ser adecuado en el caso concreto, o cuando el cumplimiento de un contrato, incluida la prestación de un servicio, sea dependiente del consentimiento, aun cuando este no sea necesario para dicho cumplimiento."*[12]

El consentimiento debe ser demostrable por parte del responsable del tratamiento, y ser específico para cada uno de los tratamientos de manera individualizada, en los casos de tratamiento masivo de datos, puede resultar una odisea, ya que el volumen de datos y la demostración de la procedencia legitima de los mismos puede ser algo caótico, por tanto, desde el RGPD se hace hincapié en la protección de datos por defecto y por diseño, es decir, pensar en la normativa desde el comienzo del ciclo de vida de los datos, antes incluso de recabar el consentimiento.

Continuando con el esclarecimiento del consentimiento en el encuadramiento del nuevo RGPD, llegamos al apartado de los artículos, los cuales conforman buena parte del Reglamento. El Artículo 6[13] del RGPD. Licitud del tratamiento, señala las pautas, indicando las condiciones para poder desarrollar el tratamiento de datos. El consentimiento es clave en la protección de datos, ya que permite respetar la autonomía de los interesados y poder tratar los datos de manera transparente. Este consentimiento, es de suma importancia, ya que, hoy en día, las nuevas tecnologías han englobado el tratamiento de datos, y se necesita un marco regulatorio que ponga control sobre el trasvase libre de datos personales.

La base para un tratamiento de datos personales conecta directamente con un consentimiento informado e inequívoco lo cual es un gran avance en nuestra sociedad, con el cambio de normativa, hemos sufrido un verdadero bombardeo de correos electrónicos de numerosas empresas intentando recabar el consentimiento, ya que antiguamente con la antigua LOPD de 1999, este se presuponía simplemente por navegar en la red como tácito. Es decir, si navegabas

[12] Ídem. Considerando 43.

[13] Ídem. Artículo 6.

por una determinada página web, esta entendía que dabas tu visto bueno a ceder tus datos personales al responsable del tratamiento de dicha *website*.

Esto ha cambiado radicalmente con la llegada del RGPD y la nueva LOPDGDD. Ahora el consentimiento como hemos podido observar sufre un cambio en la nueva reglamentación, este no es un cambio banal, el responsable debe demostrar que ha obtenido este consentimiento, en consecuencia, parece evidente y sensato que todo responsable de un tratamiento, si quiere utilizar el consentimiento del interesado para un tratamiento de datos personales, querrá cubrirse las espaldas ante posibles infracciones y sus más que probables sanciones de la AEPD o en el caso de otro países autoridades de control de esos otros estados.

El Big Data se nutre de cantidades masivas de datos, las posibilidades son infinitas y los campos a explorar irán progresando paulatinamente, la clave radica en utilizar los datos personales (si existieran) con responsabilidad y lealtad.

Permaneciendo en la línea de cómo demostrar este consentimiento por parte del responsable, tenemos el artículo 7[14] del RGPD, condiciones para el consentimiento, el cual nos expresa la obligación del responsable de demostrar que obtuvo el consentimiento del interesado, y que este conoce su derecho a retirar su consentimiento en cualquier momento. Ya no es válido el consentimiento tácito, si se tratase el caso de una obtención online del consentimiento, la aceptación por parte de un clic en una política de privacidad se entiende como consentimiento valido, siempre y cuando las casillas no estén premarcadas, y exista una casilla para cada consentimiento. Como por ejemplo el envío de publicidad.

El Reglamento es muy claro al respecto, y este es un punto muy importante para el tratamiento de datos, hay que diferenciar cada consentimiento con su finalidad dada, y que la facilidad de revocamiento sea también igual de sencilla. Esto choca frontalmente con la esencia del Big Data, que busca la reutilización de los datos personales en una variedad de campos inimaginables, utilizando los datos para usos secundarios, la rigidez de la legislación en esta materia es claramente una barrera. ¿Deberían los responsables de tratamiento, conseguir un

[14] Ídem. Artículo 7.

consentimiento informado, inequívoco y revocable cada vez que traten los datos con una finalidad diferente? La respuesta es afirmativa, cada nueva finalidad necesita el consentimiento expreso del interesado. La normativa en el Espacio Económico Europeo es sumamente rígida y choca frontalmente con la utilizada en países de América como Estados Unidos o Canadá u asiáticos como Japón o China.

La normativa nacional (LOPDGDD) viene a decir lo mismo, sin ningún cambio en su artículo 6: *"Tratamiento basado en el consentimiento del afectado. ... Cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectado para una pluralidad de finalidades será preciso que conste de manera específica e inequívoca que dicho consentimiento se otorga para todas ellas…"*[15]

La Ley Orgánica de Protección de Datos y Garantías de los Derechos Digitales, es la encargada de desarrollar el reglamento europeo en nuestro país, en lo referente al consentimiento, se refiere en los artículos 6 (Tratamiento basado en el consentimiento del afectado) y artículo 7 (Consentimiento de los menores de edad).

La legislación a nivel nacional y europea funciona en concordancia, la LOPDGDD intenta desarrollar el RGPD, aunque no aporta casi nada nuevo al mismo, el consentimiento es una base legitimadora para utilizar datos personales eficaz y cristalina, pero deja patente la obligación de cumplir con varias premisas. Entre ellas un consentimiento para cada tratamiento de datos, lo cual hace que, en el ámbito del Big Data, esta base legitimadora sea residual, ya que la ventaja del Big Data es el tratamiento de datos con diferentes finalidades.

Algunas empresas como Movistar[16] en su política de privacidad informan que utilizan el consentimiento expreso para tratar datos personales para envíos masivos de publicidad o tratar datos de clientes, productos o servicios con el fin de crear perfil comercial para proveedores. El consentimiento expreso para estos tratamientos de datos es fácil de recabar y fáciles de omitir posteriormente, porque la finalidad es única. La forma de hacer fácil este consentimiento

[15] Artículo 6. LOPDGDD, Boletín Oficial del Estado. Disponible en: https://www.boe.es/boe/dias/2018/12/06/pdfs/BOE-A-2018-16673.pdf. Referencia: 17 de diciembre de 2018.

[16] Política de privacidad de Movistar. Movistar. Disponible en: http://www.movistar.es/particulares/centro-de-privacidad/ Referencia: 7 de marzo de 2019.

expreso es basándose en la protección por defecto y por diseño, donde se puede aceptar este tipo de prácticas cuando creamos la cuenta online o similares, administrando quien acepta este tipo de tratamiento de datos, o quien lo rechaza actualizando la base de datos de envió de marketing a diario.

Respecto a los menores podemos recalcar a nivel normativo el considerando 38[17] del RGPD, por el cual se origina la idea de que los menores necesitan una protección específica de sus datos personales por sus vulnerabilidades evidentes en la toma de decisiones, esta protección es especialmente necesaria para fines de mercadotecnia o para la elaboración de perfiles.

Esta protección específica del considerando 38, es un factor diferenciador en materia de protección de datos, la utilización del Big Data con fines de mercadotecnia se está dando hoy en día. Lo que conlleva a un esfuerzo mayor en la protección y en la captura de estos datos a fin de evitar el tratamiento de menores por error o sin el consentimiento de los padres/tutores legales.

El tratamiento de datos en menores de edad es un tema delicado, la normativa española en su artículo 7[18] de la LOPDGDD (consentimiento de los menores de edad), fija que, para mayores de catorce años, su tratamiento es permitido con el consentimiento del menor cuando su consentimiento sea expreso e informado, con un lenguaje coloquial para que cualquier menor de esa edad pueda comprender las consecuencias de este tratamiento. Y en el caso de menores de catorce años, con el consentimiento del titular de la patria potestad o tutela.

Hay que tener en cuenta que el tratamiento de datos de menores de edad es un riesgo para ellos, existe un peligro ya que están en una etapa de formación de la personalidad, y desarrollo. El Big Data puede ser una herramienta peligrosa en casos como la elaboración de perfiles y la publicidad personalizada, que pueden influir en sus ideas perjudicando su desarrollo, debido a lo cual, hay que ser cautelosos a la hora de utilizar el Big Data y datos de menores de edad.

[17] Considerando 38. RGPD, Boletín Oficial del Estado. Disponible en: https://www.boe.es/doue/2016/119/L00001-00088.pdf Referencia: 11 de febrero de 2019.

[18] Artículo 7. LOPDGDD, Boletín Oficial del Estado. Disponible en: https://www.boe.es/boe/dias/2018/12/06/pdfs/BOE-A-2018-16673.pdf. Referencia: 11 de febrero de 2019.

## VII.2. Interés Público.

El artículo 6. e del RGPD, especifica que los tratamientos de datos en misión del interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento es una base legitimadora. Por tanto, nos encontramos ante un nuevo abanico de posibilidades para el Big Data en las administraciones públicas.

Este fenómeno podríamos enmarcarlo en el concepto de las *Smart Cities*, las administraciones tienen una doble base legitimadora para realizar tratamientos de datos personales, no solo pueden basarse en el artículo 6.e del RGPD si no, que pueden reforzarse en el artículo 6.c el cual indica que el tratamiento es licito en base a una obligación legal aplicable al responsable del tratamiento. Existe cierta controversia ante este hecho, ya que las administraciones publicas parten con una ventaja mayúscula en el tratamiento de datos personales, la AEPD tiene potestad para aplicar sanciones cuantiosas ante el tratamiento de datos de manera irregular, ya sean sanciones leves o incluso graves con una cuantía que puede llegar al 4% de la facturación de la empresa o hasta veinte millones de euros[19]. En cambio, el rango normativo de reglamento deja desarrollar por la legislación nacional esta base, y la LOPDGDD en su artículo 77.3 establece que serán sancionadas con apercibimiento las administraciones públicas, pero sin sanciones económicas. De esta manera queda patente que no existe una medida correctora en caso de abuso en sus funciones de las administraciones. Esta defensa es positiva para las arcas del estado, pero debería ser más estricta con las personas responsables de estos posibles fallos, más allá de procedimiento disciplinario a la persona responsable.

La controversia está servida, ya ocurrió con el apercibimiento al Ministerio de Justicia por una infracción en su sistema Lexnet[20] donde usuarios pudieron acceder a los datos de otros por un fallo en el sistema informático, la LOPD de 1999 podía sancionar o advertir a las administraciones, pero no podía poner multa. Sí hubiese sido una empresa privada la multa podría haber ascendido a tres cientos mil euros.

[19] Artículo 83.5. RGPD, Boletín Oficial del Estado. Disponible en: https://www.boe.es/doue/2016/119/L00001-00088.pdf Referencia: 20 de febrero de 2019.

[20] La AEPD concluye que el Ministerio de Justicia se saltó la Ley de Protección de Datos con LexNet. Facua. Disponible en: https://www.facua.org/es/noticia.php?Id=12662. Referencia: 5 de marzo de 2019.

Esta desigualdad, puede ser entendida a favor de los ciudadanos y de las arcas públicas, pero se deberían tomar medidas más estrictas de control en futuras ocasiones, en el caso del tratamiento de datos masivo del Big Data, se entiende que la administración pública ejerce un tratamiento a favor de los ciudadanos analizando los datos para dar valor a los mismos, tenemos ejemplos claros en las ciudades inteligentes, que recaban datos no personales como el transporte urbano, con sensores, cámaras de video vigilancia, paradas de autobús, recarga de tarjetas de transporte.. o en el urbanismo e infraestructuras de las ciudades, cultura y ocio, o medio ambiente para medir los niveles de residuos en contenedores, contaminación en el aire o polen para dar servicio de información a los alérgicos.

Los datos no personales, no entran dentro de la normativa, LOPDGDD y RGPD, pero existe un riesgo de relacionar datos personales con datos no personales, como el caso de censo de la población, consumo de agua asociado a los ciudadanos, consumo de la luz, raza, sexo, edad de la población… Todos estos datos son analizados de manera masiva, un país necesita tratar estos datos para llevar un control de este, aplicar políticas o controlar sus presupuestos. Por lo cual, las administraciones deberían hacer una introspección de si los datos están siendo minimizados para cumplir con la normativa y la finalidad buscada, que no es otra que analizar los datos para finalidades específicas y defender a la vez la defensa de la intimidad de las personas, un derecho constitucional de nuestro artículo 18.4 CE.

Un ejemplo de cómo tratar los datos masivos de manera correcta es el *"Transport for London, TfL",* la empresa de transporte de Londres controla autobuses, trenes, taxis, carreteras, carril bici, ferry... Tiene datos no personales y a la vez datos de una gran cantidad de usuarios que utilizan el servicio público de transporte todos los días. Hablamos de millones de personas en una de las ciudades más importantes del mundo.

Lauren Sager Winstein, jefe del equipo de análisis de datos de TfL, explica[21] en el libro de Bernard Marr "45 casos de éxito reales de uso del Big Data": *"Usamos el Big Data para conocer como los consumidores utilizan el transporte público y que necesitan del transporte*

[21] MARR, B. (2016: 223-228).

*público. Con esto en mente, tenemos dos objetivos prioritarios al recolectar información y analizarla, planificar mejores servicios y devolver información valiosa a los usuarios"*

La utilización del Big Data por parte de la empresa londinense se basa en tres bases diferentes, la primera es registrar el trayecto programado de cada usuario, gestionar eventos imprevistos como nevadas o accidentes y finalmente proveer información personalizada a cada usuario. Todo esto lo hace sin usar datos personales de las personas, lo cual es un gran logro al tratarse de un tratamiento masivo de datos, lo consigue porque los usuarios utilizan tarjetas con numeración específica, anonimizando a los ciudadanos. Un claro ejemplo de utilización de las tecnologías en consonancia con la normativa.

Estas tarjetas son usadas desde 2003, el llamado *"Oyster smartcard ticketing system"* (en adelante, *Oyster*). Estas tarjetas proveen a TfL de una cantidad masiva de datos todos los días. Los ciudadanos londinenses o turistas que las utilizan para entrar y salir de autobuses o trenes pueden incluso utilizar tecnología RFID y pagar con sus teléfonos móviles. El sistema *Oyster* genera 19 millones de entradas y salidas cada día que pueden ser analizados[22].

Desde la entrada del Big Data en TfL, es posible analizar la cantidad ingente de datos que puede generar la ciudad de Londres, cómo las personas viajan en metro, tranvía, tren o autobús. Por poner un ejemplo, la empresa pública conoce analizando estos datos, las paradas más transitadas, la época del año con más turistas o los meses con la red en picos de servicio y poder actuar, redireccionando el transporte en tiempo real para evitar incidencias, todo este análisis no era posible hace años. La empresa incluso puede tramitar directamente las devoluciones de tiques si se demora su llegada más de 15 minutos, si existiera una denuncia, ésta es estudiada y gracias a los sensores de los transportes, sumados a la tecnología RFID de los tiques y los datos externos de tráfico, clima, etc.., hace posible que TfL pueda resolver favorable o negativamente estas reclamaciones basándose en criterios objetivos de porque ha ocurrido el retraso de manera automática.

[22] Ídem. (223-228).

Wenstein incluso comenta un caso real en este mismo artículo del libro de Bernard Marr: el cierre del puente Putney por obras en 2014. Este hecho afectaba a más de ciento diez mil viajes por semana, trabajaron desde la empresa pública basándose en los datos masivos recolectados previos a la obra, y tomaron decisiones en base a ellos, decidieron mantener abierto el puente a ciclistas y peatones, conociendo que la mitad de los viajes en esa ruta terminaban cerca del puente o empezaban allí. Para solventar el problema de la otra mitad de los viajeros asiduos, se añadieron puntos nuevos de transporte y se incrementaron las rutas alternativas de autobuses en las cercanías del puente, sumando a este esfuerzo extra, también enviaron emails a los damnificados, informando de las nuevas rutas y ubicaciones de las nuevas paradas. Los usuarios de TfL respondieron a una encuesta posterior, donde un 83% de ellos expresaron su satisfacción al igual que la información recibida fue útil o incluso muy útil para planificar su día a día.

Los datos recabados por las administraciones, de la población, domicilio, edad… Pueden ser devueltas como valor añadido de una forma excelente como el funcionamiento de las *Smart Cities*, el tratamiento de datos debe ser llevado a cabo de una manera eficaz y anónima en la manera de lo posible como en TfL. De esta manera la base legitimadora es totalmente correcta con el Big Data, de la forma en que al dar un valor utilizando estos métodos a los ciudadanos se hace de una manera responsable como con las tarjetas anónimas de transporte.

Es importante darse cuenta de que vivimos en un mundo globalizado y que los datos, tienen utilidades presentes y podrán tener utilidades futuras no previstas hoy en día, incluso si viviéramos aislados en la montaña, nos veríamos involucrados en el devenir de nuestra sociedad tecnológica de alguna forma directa o indirecta en algún momento. Es imposible aislarse del devenir futuro, el cambio está aquí y debemos cooperar a que sea positivo entrelazando la intimidad personal y los servicios públicos de una manera equilibrada y sostenible.

## VII.3. Interés Legítimo.

Esta base legitimadora es utilizada como una manera de solución por grandes empresas, a la nueva regulación de protección de datos a nivel europeo. El tratamiento masivo de datos en entornos de Big Data no tiene demasiadas bases legitimadoras, se entiende que el interés público u obligación legal en el sentido de las administraciones públicas, sea un criterio coherente como validez, las grandes empresas que tratan datos masivamente tienen un problema

con la nueva regulación, el consentimiento expreso para varios tratamientos es una utopía, con la nueva regulación como hemos visto anteriormente, se necesita un consentimiento expreso para cada nuevo tratamiento de datos, el Big Data busca encontrar valor de nuevas finalidades de datos, cuando los datos parece que no aportan nada nuevo, el Big Data encuentra la forma de aportar un extra, este supuesto es contrario a la búsqueda del consentimiento como base legitimadora, por tanto en esta búsqueda de entrar dentro de la ley se encuentra el Interés Legítimo.

El artículo 6.f del RGPD, indica que el tratamiento es necesario para la búsqueda de intereses legítimos perseguidos por el responsable del tratamiento, en esta base se argumentan la mayoría de las empresas en su búsqueda de dar un mejor servicio al cliente basándose en una especie de quid pro quo, por la cual las empresas tratan datos para aconsejar a los clientes productos recomendados, o dar un mejor servicio.

El uso del Big Data es beneficioso para empresas, un ejemplo es Amazon (Amazon.com, Inc.), desde hace años tiene un modelo de negocio de venta online, el cual, debido a su increíble éxito, ha permitido diversificar su negocio en nuevos campos como el desarrollo de series de tv y plataformas de *streaming*, de música y contenido audiovisual. La pregunta es sencilla, ¿cómo ha obtenido tanto éxito?

La respuesta es el uso de la tecnología Big Data, que ha ayudado a la gigante americana de Seattle. Esto se debe a su tecnología de predictibilidad en las compras de los usuarios, Amazon ha evolucionado desde ser una empresa de venta y distribución, a volverse una empresa con productos propios, el crecimiento es increíble. Esta herramienta de predictibilidad se basa en tratar los datos de compras y de "Listas de Deseos" (posibles futuras compras), de los usuarios de Amazon para ofrecerles productos similares, con el gran abanico de productos que vende y la volatilidad de precios y ofertas, puede predecir cuándo compraran los usuarios y que determinados productos, todo ello a través del estudio y análisis del Big Data. Incluso hoy en día vende herramientas para tratar datos en empresas a través de su *Web Amazon Services*, para implementar la tecnología Big Data en tu propio negocio con su asesoramiento y servicio su Cloud.

Dentro de esta empresa, otro caso conocido[23], es la compra en 2009 de Zappos (tienda online de venta de zapatos), esta compra fue estratégica, mejoro mucho a Amazon. Zappos era conocida como la mejor compañía en atención al cliente post venta, Amazon instauro este modelo al adquirir a la empresa. Zappos usaba los datos históricos de sus clientes para hacerles marketing especifico y programas de fidelización personalizados y Amazon se aprovechó de esta adquisición para también mejorar sus sistemas post venta.

Este ejemplo enlaza muy bien en como una simple transacción de compra, puede derivar en valor añadido si se utilizan estos datos en otros campos. El dato interesante, es que la publicidad basada en productos similares comprados por clientes puede estar basada en la compraventa del producto y basarse en la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (en adelante, LSSI), en su artículo 21, por el cual establece que si existiera una relación contractual previa (la venta de un producto), no sería necesaria la obtención del consentimiento expreso para recibir publicidad siempre y cuando fuesen productos similares a los comprados previamente. Por tanto, el servicio postventa esta correctamente realizado, el quid de la cuestión es basarse en el interés legítimo para recomendar productos en base a "listas de gustos", ya que ni siquiera son productos adquiridos.

Otro caso similar es el de Airbnb, empresa también mundialmente conocida, ya que nació de la nada en 2008, y ahora es una de las más importantes a nivel mundial para cualquier viajero. La empresa ha ido guardando datos sobre preferencias de clientes y hábitos durante las vacaciones. Con más de un millón y medio de reservas[24], treinta y cuatro mil ciudades donde el usuario puede encontrar alojamientos, y cincuenta millones de clientes, Airbnb, posee entre uno y medio, a dos, Petabytes de datos totales para poder analizar.

La empresa de San Francisco utiliza estos datos utilizando tecnología Big Data de diversas formas, desde para poder conocer los picos de demanda, por meses, ciudades/pueblos más demandados, los precios por zona y época del año, hasta para aconsejar/recomendar a los dueños de los apartamentos un precio de mercado idóneo en su zona o las mejoras pertinentes

[23] MARR, B. (2018: 24-27)

[24] MARR, B. (2016: 163-167).

necesarias en cada apartamento según la demanda de los usuarios (ejemplo Wifi, dos juegos de llaves, entrada con código al domicilio...).

Airbnb, centraliza sus esfuerzos en conseguir apartamentos en destinos populares durante épocas de vacaciones, los algoritmos que utilizan para aconsejar precios de habitaciones o apartamentos se basan en opiniones post alojamiento de los usuarios, tales como lo más demandado del apartamento o cosas a mejorar. Hay que tener en cuenta, que, dependiendo de la ciudad, país o época del año, quizás los clientes buscaran diferentes comodidades, como ejemplo, una persona no buscara un apartamento con piscina en Moscú en pleno invierno. Pero quizás es un requisito útil en la sierra de Madrid para una casa en verano. La evolución tecnológica es imparable, lo que antiguamente era una reserva de hospedaje, ha derivado en un análisis exhaustivo de las preferencias de los huéspedes y ofrecerles las mejores comodidades amoldándose a sus gustos. Basándose en el interés legítimo de este tratamiento de datos para darles un servicio más personalizado, como podemos observar en su política de privacidad:

*"Usted puede facilitarnos datos personales adicionales para obtener una mejor experiencia de uso al utilizar la Plataforma de Airbnb. Esta información adicional será procesada en base a nuestro interés legítimo o, cuando corresponda, a su consentimiento.*

*Información adicional de perfil. Usted puede proporcionar información adicional como parte de su perfil de Airbnb (como su sexo, idioma(s) preferido(s), ciudad y una descripción personal). .....*

*Información de contacto de agenda. ....*

*Otra información..."*[25]

Las empresas dan sus opciones y se cubren alegando que la realización de una acción está basada en el interés legítimo para poder asociar estos datos a nuestro perfil, al consentimiento de las personas "expreso" al realizar las acciones voluntariamente, de esta forma las empresas se saltan el RGPD relacionado a la elaboración de perfiles prohibida[26] del RGPD y solo validada

[25] Política de privacidad de Airbnb. Airbnb. Disponible en: https://www.airbnb.es/terms/privacy_policy. Referencia: 8 de marzo de 2019.

[26] Artículo 22. RGPD, Boletín Oficial del Estado. Disponible en: https://www.boe.es/doue/2016/119/L00001-00088.pdf Referencia: 8 de marzo de 2019.

por el tratamiento basado en un contrato, consentimiento expreso o en el cumplimiento de una ley. De esta forma pueden realizar elaboraciones de perfiles anonimizando nuestros datos, basándose en las bases legitimadoras anteriormente expresas.

La controversia radica en que, la nueva normativa busca proteger a los usuarios, y busca que estén informados de una manera clara y que comprendan los tratamientos de datos a los que son sometido, incluso se puede dar la información por capas para facilitar/resumir estas finalidades, quizás es un problema de educación, el cual aboga por que los servicios tienen que ser inmediatos y no se da importancia a las consecuencias. Pero las grandes empresas como Airbnb o Amazon tienen el poder suficiente como para imponer sus políticas en términos de privacidad ante los individuos, incluso hacer sus políticas de privacidad confusas y sumamente en farragosas. Quizás las autoridades de control europeas deberían tomar parte en que las empresas cumplan la información que facilitan a los usuarios de manera más sencilla.

## VII.4. Cumplimiento de un contrato.

El Big Data con la base legitimadora del cumplimiento de un contrato, artículo 6.b del RGPD, podría basarse en el tratamiento masivo de datos con finalidades de mercadotecnia, en el caso de contratos de compra venta, entrando en el marco de la LSSI, o en el caso del cumplimiento de un servicio contratado como pudiera ser el tratamiento de los datos de los clientes para la red de telecomunicaciones de una empresa como Movistar.

El problema radica en que cuando los datos van a ser tratados con otras finalidades diferentes entramos en el “limbo” normativo, que nos lleva a salirnos de los tratamientos necesarios para el contrato, el objetivo del nuevo RGPD es la búsqueda de la minimización en la utilización de los datos personales, es decir, realizar tratamientos de datos en post del contrato no resulta muy correcto, aquí es donde se junta la rueda de las bases legitimadoras, consentimiento expreso (residual y casi utópico para Big Data) e interés legítimo relacionado con los actos voluntarios como añadir datos extras o basándose en la mejora de la calidad del servicio como vimos previamente.

Analizando la política de privacidad de varias empresas, la mayoría de las veces tratan de buscar la legitimización de sus tratamientos en varias bases legales, sin dejar claro en qué base legal están sustentadas, si en el contrato, si en el consentimiento expreso del usuario o en el interés legítimo. Podríamos analizar que el tratamiento de datos para cumplir un contrato, son meramente los datos para la realización del servicio, es decir, datos bancarios para facturación, nombre, dirección, ip, conversaciones con atención al cliente y similares.

No se entiende que, en el desarrollo del servicio, se necesitasen datos fuera de lo "común" para la consecución de este, partiendo de la minimización de los datos, por tanto, el Big Data no encuentra una base sólida en el contrato para la realización de tratamientos de datos con la búsqueda de valor añadido. Todo lo que exceda estos tratamientos, entra en el círculo del consentimiento expreso e interés legítimo. Todo en sí mismo es algo confuso, ya que se entiende que el tratamiento de datos para ofrecer un servicio conlleva en muchos casos, un estudio del servicio prestado para una mejora del mismo, pero este estudio de los datos debería hacerse anónimamente o habiendo informado de manera concisa y clara, de este hecho se aprovechan las empresas para "enlazar" el contrato con el interés legítimo, y hacer uso de tratamientos de datos diversos dentro del reglamento.

## VII.5. Obligación legal.

El análisis de datos masivos para cumplir con una ley es uno de los tratamientos de datos en entornos de Big Data más favorables para los ciudadanos, hoy en día, es muy común observar como las ciudades europeas abren al público bases de datos llamadas "Open Data" para que los ciudadanos puedan hacer uso de estos datos en beneficio propio, los estados controlan cantidades ingentes de datos, los datos más personales son de conocimiento del estado.

El tratamiento de estos datos por su parte responde a un interés público, y a una obligación legal, la obligación legal de los estados para tratar datos se refiere al artículo 6.c del RGPD, y artículo 8 LOPDGDD, que imponen como una base legitimadora el cumplimiento de una obligación legal.

Es cierto que los estados analizan los datos, ya que son, a fin de cuentas, "empresas" grandes, donde tienen que dar unos servicios a los ciudadanos a razón de los impuestos que les pagan, la previsión ante el futuro es un paso vital para los estados, prever en sus políticas, la edad de los ciudadanos o la mortalidad de los mismos.

Estos datos se analizan normalmente anonimizados para que no puedan ser identificados los ciudadanos, pero el tratamiento de datos en base a una obligación legal más interesante es el Big Data utilizado en pro de la salud pública.

Existen categorías especiales de datos *"aquellos datos que, de divulgarse de manera indebida, podrían afectar a la esfera más íntima del ser humano, tales como ideología, afiliación sindical, religión, creencias, origen racial o étnico, salud y orientación sexual."*[27]

El RGPD añade a la descripción del libro de Elena Gil, los datos genéticos y datos biométricos a esta categoría especial de datos, en la antigua normativa, se les nombraba como "datos especialmente protegidos". El artículo 9[28] del RGPD nos prohíbe el tratamiento de determinados tipos de datos, tales como los datos que revelen origen étnico o racial, opiniones políticas, convicciones religiosas, afiliación sindical, datos genéticos, biométricos, relativos a salud, vida sexual, orientación sexual.

Pero esta prohibición queda levantada en algunos supuestos, como, si fuera necesario para proteger los intereses vitales del interesado o de otra persona física, cuando esté incapacitado para dar su consentimiento o por razones de interés público en el ámbito de la salud pública o asistencia sanitaria…fines de archivo en interés público, investigaciones científicas, históricas o estadísticas. La LOPDGDD sigue en la misma línea en su artículo 9[29].

[27] GIL GONZÁLEZ (2015:122).

[28] Artículo 9. RGPD, Boletín Oficial del Estado. Disponible en: https://www.boe.es/doue/2016/119/L00001-00088.pdf Referencia: 11 de febrero de 2019.

[29] Artículo 9.1. LOPDGDD. Boletín Oficial del Estado. Disponible en: https://www.boe.es/boe/dias/2018/12/06/pdfs/BOE-A-2018-16673.pdf Referencia: 11 de febrero de 2019.

En lo respectivo al sector salud, cabe resaltar que las posibilidades del Big Data en este ámbito son llamativas y muy esperanzadoras, la cantidad de datos heterogéneos que arrojan información variada sobre pacientes, sus formas de vida, enfermedades, países, puede resultar muy útil para los profesionales del sector.

Las historias clínicas electrónicas, la nutrición, dispositivos móviles, telemedicina, pruebas. Todo ayuda a solventar problemas sanitarios y luchar contra enfermedades aun sin cura o mejorar los métodos actuales, en beneficio de los pacientes. La base legitimadora de la legislación vigente para datos de salud y en nuestro caso para entornos de Big Data del artículo 9,2 RGPD abarca varias leyes según la nueva LOPDGDD en su disposición adicional decimoséptima[30] (tratamientos de datos de salud), como la Ley General de Sanidad, Ley de Prevención de Riesgos Laborales…

Ya que la utilización de los tratamientos de datos de categorías especiales será necesaria para fines de asistencia sanitaria, el Big Data utilizado con fines médicos es muy beneficioso para la sociedad, podría ser una gran ayuda ante enfermedades que aún se desconoce su funcionamiento al correlacionar datos de pacientes a nivel país, o unión europea, para buscar similitudes y diferencias.

Las técnicas de Big Data pueden ser de gran ayuda para entender los genes y como interactúan enfermedades como el cáncer o el Alzheimer. Gracias al tratamiento masivo también se puede estudiar los efectos secundarios de medicamentos, y utilizar esta información para configurar tratamientos a medida que optimicen los resultados y minimicen los riesgos.

Dentro de este tratamiento de datos, existen ya varias plataformas a nivel europeo que intentan apoyar la normativa en protección de datos y a la vez el avance en materia de compartición de información en la lucha contra enfermedades raras, el considerando 135 del RGPD, establece que los datos pueden ser utilizados con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, cumpliendo unas medidas de seguridad,

[30] Ídem. Disposición adicional décimo séptima.

como en el caso de los datos de salud, la seudonimización. Algunas de las plataformas donde se comparten estos datos en beneficio de la investigación son:

Elixir[31]: *"infraestructura europea de bioinformática, iniciativa única y sin precedentes que consolida los centros de investigación, servicios y recursos bioinformáticos de cada país de manera conjunta."*[32]

Elixir entra dentro del programa europeo de financiación 2014-2020, *Horizon* 2020[33] que financia actualmente programas de investigación a nivel europeo de diversa índole, Elixir es uno de los tres programas principales a nivel europeo, con la idea de crear una infraestructura de compartición de datos en materia de investigación científica.

Hay más de quinientos mil científicos en Europa conectados a la red de Elixir, la bioinformática necesita nutrirse de datos personales como es el caso según el RGPD de los datos genéticos.

Otra base de datos a nivel europeo que lucha en el beneficio de la investigación y curación de enfermedades raras es la plataforma: *European Platform on Rare Disease Registration* (en adelante plataforma EU RD).

La plataforma EU RD[34], está en pleno lanzamiento, a comienzos de 2019 aún está en proceso la información pertinente en su página web, este novedoso sistema que intenta luchar contra las enfermedades raras a nivel europeo, la infraestructura que se pretende utilizar, es la compartición de casos de enfermedades raras para la lucha contra las mismas entre todos los científicos asociados, una compartición de bioinformática a nivel europeo en una lucha conjunta

[31] Plataforma Elixir. Elixir-Europe. Disponible en: https://www.elixir-europe.org/about-us/who-we-are. Referencia: 8 de marzo de 2019.

[32] Definición de Elixir. UPF. Disponible en: https://www.upf.edu/web/e-noticies/archivo/-/asset_publisher/wEpPxsVRD6Vt/content/id/2669044/maximized#.XIQLeChKhPY. Referencia: 8 de marzo de 2019.

[33] Definición de Horizon 2020. ESHORIZONTE2020. Disponible en: https://eshorizonte2020.es/que-es-horizonte-2020. Referencia: 8 de marzo de 2019

[34] Plataforma EU RD. EU-RD. Disponible en: https://eu-rd-platform.jrc.ec.europa.eu/#. Referencia: 9 de marzo de 2019.

contra estas enfermedades raras, cuanta más información se tenga en conjunto, más datos podrán tratarse para la lucha de estas enfermedades buscando patrones que puedan ser útiles.

Este mastodóntico proyecto, a simple vista parece inviable en materia de protección de datos, datos especialmente protegidos como son los datos de salud o genéticos, compartidos a nivel europeo parece una utopía, pero lo interesante es que esta infraestructura tiene una herramienta muy importante a disposición de los usuarios registrados para apoyar la privacidad de los pacientes, esta herramienta se denomina "Herramienta de seudonimización" (en adelante, EUPID), EUPID sirve para las futuras aportaciones de casos reales por parte de especialistas se ve tratada por la herramienta seudonimizando los datos personales de los pacientes de forma que se vuelvan anónimos de cara a los otros usuarios que accedan a los datos personales.

La plataforma de enfermedades raras en la unión europea será próximamente una realidad, pero mientras está en proceso de finalización podemos aventurar de que será un beneficio para los ciudadanos europeos, compatibilizando la normativa en protección de datos con la búsqueda de soluciones pioneras gracias a la investigación y compartición de información a niveles masivos.

También podríamos entender el tratamiento de datos masivos en momentos de extrema necesidad y puntual, en el ámbito sanitario, como pudiera ser un caso de pandemia mundial basándonos en la base legitimadora del interés vital[35], lo cual conllevaría hipotéticamente en que la búsqueda del interés vital de la población, chocaría frontalmente con la privacidad en el tratamiento de datos personales de los pacientes, la búsqueda de una vacuna ante una enfermedad viral podría resultar legitimo para la defensa de la vida del paciente o de otros ciudadanos por encima de la privacidad individual.

[35] Artículo 6.d. RGPD. Boletín Oficial del Estado. Disponible en: https://www.boe.es/doue/2016/119/L00001-00088.pdf Referencia: 10 de marzo de 2019.

# VIII. Anonimización y Seudonimización de los datos.

## VIII.1. Seudonimización

En la protección de los datos, otra posibilidad para hacer los datos seguros es la seudonimización. Este, es un importante factor diferenciador. Los seudónimos en protección de datos son una salvaguarda de la privacidad, que pueden paliar los riesgos del tratamiento de datos. Esta técnica, no convierte los datos personales en anónimos, este método es reversible y esto significa que es posible descubrir la identidad de las personas. La definición del RGPD es la siguiente:

*"el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional 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."*[36]

En definitiva, es el cambio de determinados atributos representativos de personas por datos en forma de seudónimo, manteniendo los datos extraídos por separado. Creando la posibilidad de vinculación, pero dificultando esta acción. Este método es utilizado en el ámbito sanitario como hemos visto previamente y es el paso más seguro para el tratamiento de datos dentro de la normativa.

Hay varios tipos de seudonimización, que intentaremos comprender en base a la siguiente.

Tabla Ejemplo

| N.º Reg. | DNI | Nombre | Edad | Sector de trabajo | Salario bruto Anual | Enfermedad |
|---|---|---|---|---|---|---|
| 1 | 74715300H | Claudia Pérez | 57 | CEO | 100.000 | Gripe |

[36] Ídem. Artículo. 4.5.

| | | | | | | |
|---|---|---|---|---|---|---|
| 2 | 76819745C | Juan Montes | 22 | Marketing | 21.000 | Gastritis. |
| 3 | 30516422G | Alicia González | 36 | Abogacía | 34.000 | Neumonía |
| 4 | 49167240V | Carlos Moreno | 45 | Enfermería | 28.000 | Cáncer de pulmón. |
| 5 | 30147735M | Elena Jiménez | 51 | Medicina | 37.000 | Ulcera Estomacal. |

*Tabla 2.. Elaboración propia.*

Algunas definiciones que debemos tener en cuenta para entender la materia:

- Identificadores directos: Característica de una persona que pueda ser identificada a la misma, nombre, dirección, número de DNI…No son de capital importancia para propósitos estadísticos o de investigación así que podrían ser eliminados a fin de conseguir la anonimización.
- Identificadores Indirectos: Atributos que pueden ser compartidos por varias personas y cuya relación puede conducir a la reidentificación de alguna de ellas.
- Atributos sensibles: En nuestro país podríamos definirlos como datos de carácter especial, están estipulados en el artículo 9 del RGPD, Tratamiento de categorías especiales de datos personales y en el artículo 9 de la LOPDGDD, Categorías especiales de datos. Algunos de estos son: Religión, afiliación sindical, política, origen racial, ideología, creencias, étnico, salud o vida sexual...

En la tabla anterior, los identificadores y atributos explicados antes serían:

• Identificadores Directos: DNI, Nombre (puede ser compartido por varias personas).

• Identificadores Indirectos: Edad, Sector de Trabajo.

• Atributos Sensibles: Salario Bruto y Enfermedad.

**Método de Cifrado de datos con clave secreta:**

Un caso de seudonimización seria aplicar una sustitución entre el nombre de la persona y DNI por un código cifrado, de esta manera solo la persona con la información que permite vincular el código al dato personal podrá identificarlo, a modo de "llave" del candado.

| | | | | | | |
|---|---|---|---|---|---|---|
| 2 | ~~**76819745C**~~ | ~~**Juan Montes**~~ | 22 | Marketing | 21.000 | Gastritis. |
| 3 | ~~**30516422G**~~ | ~~**Alicia González**~~ | 36 | Abogacía | 34.000 | Neumonía |

| | | | | | | |
|---|---|---|---|---|---|---|
| 2 | **JV#1** | **S#21** | 22 | Marketing | 21.000 | Gastritis. |
| 3 | **LM#0** | **B#85** | 36 | Abogacía | 34.000 | Neumonía |

En este ejemplo, habría una clave que solo tendría el responsable o encargado del tratamiento, por la cual podría identificar que S#21 es Juan Montes y lo mismo para las otras variables. Es de vital importancia mantener a buen recaudo la clave del cifrado, en este caso y la clave de los otros métodos también, ya que permitiría la reidentificación de manera inmediata.

Otros métodos de seudonimización, difieren en el modo de seudonimizar, pero el proceso es similar, siempre debe ser reversible y, por tanto, entran dentro del tratamiento de datos personales, otros métodos serían la función hash como en anonimización, pero de manera reversible, la descomposición en tokens o función con clave entre otras.

La complejidad respecto a reidentificación dependerá únicamente del proceso o método utilizado, y los valores o atributos sustituidos, hay que tener en cuenta que este método no es infalible, ya que, con las nuevas tecnologías, debemos tomar medidas extras de protección.

La realización de una EIPD es recomendable cuando el tratamiento de datos personales se base en datos de carácter personal, expresados como ya hemos comentado anteriormente en el artículo 9 del RGPD, Tratamiento de categorías especiales de datos personales.

## VIII.2. Anonimización

El tratamiento de grandes volúmenes de datos ofrece innumerables beneficios al conjunto de la sociedad, pero a la vez es un riesgo para la privacidad y la protección de datos personales de los ciudadanos. Por ello, la anonimización es la única solución viable para el Big Data, anonimizar los datos personales de los ciudadanos en un intento de defender su privacidad y poder seguir tratando los datos como un avance para la sociedad, evitando la normativa de protección de datos al haber convertido los datos personales en anónimos.

En este sentido, la AEPD presento una guía sobre orientaciones en el procedimiento de anonimización, que indica lo siguiente sobre este proceso: *"La finalidad del proceso de anonimización es eliminar o reducir al mínimo los riesgos de reidentificación de los datos anonimizados manteniendo la veracidad de los resultados del tratamiento de los mismos, es decir, además de evitar la identificación de las personas, los datos anonimizados deben garantizar que cualquier operación o tratamiento que pueda ser realizado con posterioridad a la anonimización no conlleva una distorsión de los datos reales."* "[37]

Por esta razón, en el proceso de anonimización se deberá producir "la ruptura de la cadena de identificación de las personas", tanto directa como indirecta (entendiéndose por identificación indirecta aquella que pueda tener lugar "como consecuencia de información de una o varias fuentes que por sí misma o en combinación de otros factores puede permitir la reidentificación de las personas cuando sus datos hubieran sido anonimizados. Por ejemplo, la combinación de sexo, edad, lugar de nacimiento y padecimiento de una determinada enfermedad pueden permitir la identificación indirecta de una persona concreta").

En el diseño del proceso de anonimización será necesario prever las consecuencias de una eventual reidentificación de las personas que pudiera generar un perjuicio o merma de sus derechos. Igualmente será necesario prever una hipotética pérdida de información por

[37] Orientaciones y garantías en los procedimientos de anonimización de datos personales. AEPD. Disponible en: https://datos.gob.es/sites/default/files/doc/file/orientaciones_y_garantias_anonimizacion_0.pdf. Referencia: 10 de diciembre de 2018.

negligencia del personal implicado, por falta de una política de anonimización adecuada o por una revelación de secreto intencionada que diera lugar a la pérdida de las variables de identificación o claves de identificación de las personas.

La anonimización consiste en la ruptura de la cadena de identificación de las personas, es decir, volver anónimos los datos personales. Esta es la principal solución al tratamiento de datos personales en el ámbito del Big Data, la regulación avanza más despacio que las nuevas tecnologías y esto incide de primera mano en el Big Data, es una materia nueva para casi todos, pero ha llegado para quedarse, por tanto, hay que buscar un encuadre que satisfaga a la regulación y a los avances tecnológicos.

Hay que resaltar que la obtención de los datos personales a anonimizar tiene que cumplir con la normativa vigente en Protección de Datos. Siempre y cuando no se recabasen directamente anónimos. Esto es un hecho importante a tener en cuenta, ya que, aunque intentemos evitar la normativa, siempre hay que tener en cuenta su influencia. Aparte de que según informe de la AEPD y del grupo de trabajo del artículo 29, anonimizar propiamente, es un tratamiento de datos. Detalle que veremos más adelante.

El miedo que siente la población ante las posibles invasiones de su privacidad podrían ser fundadas, ya que hoy en día se tratan datos personales continuamente, smartphones, tablets, ordenadores, asistentes virtuales inteligentes, domótica en casa… Quizás la mejor manera de buscar el equilibrio entre las utilidades informáticas (o de otra índole) que utilizan el tratamiento de datos para dar un beneficio y la privacidad de los individuos en el tratamiento de sus datos personales sea la anonimización.

Lo que se pretende en el ámbito del Big Data con datos personales anonimizados, no es más que un Big Data con privacidad, la búsqueda de una forma que no sea desorbitada en recursos, entre la unión de la tecnología y la legislación, que no es otra que la defensa de la intimidad personal de los ciudadanos y la búsqueda de beneficio para los mismos cumpliendo con la normativa vigente.

La anonimización no es un procedimiento sencillo, se puede hacer de varias maneras explicadas posteriormente, pero para un logro eficaz, deberíamos basarnos en la privacidad desde el diseño de la cual nos marca el RGPD en el artículo 25, pensar en la privacidad desde el comienzo es lo mismo a construir una casa desde las bases y no por el tejado.

Podríamos definir este concepto dentro del ámbito de la llamada privacidad proactiva (antes de), en vez de reactiva (después de), para poder hacerla efectiva de manera eficiente. El ciclo de vida del dato empieza desde la captura de los datos y la información a los interesados, los integrantes del proceso del ciclo de vida del dato deben estar formados de su cometido en todo momento, siguiendo el principio de formación e información. Cuando vamos a realizar un proceso de anonimización, los riesgos a los que estamos expuestos son notables, hay que tener en cuenta que, según la normativa, un dato anonimizado NO es un dato personal[38], por tanto, evitaríamos la normativa de protección de datos.

¿Cómo lograr la anonimización? Para lograr la anonimización, el primer paso es crear un procedimiento de actuación, el cual servirá de base a los involucrados para realizar correctamente el proceso, y será necesario una Evaluación de Impacto (En adelante EIPD), para evaluar los riesgos previa anonimización a fin de minimizar posibles errores que lleven a la reidentificación.

Hoy en día el volumen de información pública gracias a las redes sociales, datos abiertos... es incontable, relacionar datos anonimizados con personas identificables no es ninguna situación descabellada. Toda previsión es poca. La realización de la EIPD conllevaría un análisis exhaustivo de los pros y contras del proceso de anonimización muy positivo para ver la viabilidad del proceso.

Para definir el proceso, podríamos decir que consiste en diferenciar cuales son los identificadores potenciales y modificar estas variables para reducir el riesgo de reidentificación. Hay que tener en consideración las últimas técnicas de Big Data que correlacionan datos y

[38] Dictamen 04/2007. GT29, CE. (Concepto de datos personales).

pueden llegar a des anonimizar datos personales. Por tanto, este proceso debe hacerse de manera segura y responsable.

Hay diversos métodos de anonimización, pero utilizaremos un ejemplo entendible de manera fácil para comprender la finalidad. Imaginemos que estamos haciendo un estudio sobre el puesto de trabajo, salario y enfermedades, buscando correlaciones.

**Método basado en reducción de datos.**

El método de reducción se basa en la reducción o eliminación de variables con la finalidad de minimizar las posibilidades de identificación, a menor número de datos personales, menor será la posibilidad de identificar a los individuos.

**Supresión / Eliminación de variables:** Consiste en eliminar los identificadores directos. Esta técnica afecta a la utilidad de los datos, pero, por el contrario, si estos datos no tuviesen relevancia a la hora del análisis podría ser una manera óptima.

| | | | | | | |
|---|---|---|---|---|---|---|
| 4 | ~~**49167240V**~~ | Carlos ~~**Moreno**~~ | 45 | Enfermería | 28.000 | Cáncer de pulmón. |
| 4 | ********* | Carlos ***** | 45 | Enfermería | 28.000 | Cáncer de pulmón. |

La simpleza de este método es positiva a nivel organizativo, pero consiste un déficit respecto a mantener la información. El DNI era el dato más significativo a nivel identificativo, su eliminación es clave para la anonimización.

En el caso de que el campo de numero nacional de identidad fuese imprescindible, este método no podría utilizarse.

**Supresión/ Eliminación registros:** Es la eliminación total de todos los datos personales en la base de datos, utilizado en casos extremos.

**Recodificación global de datos:** Es útil para datos numéricos, se trata en generalizar en categorías menos específicas.

| | | | | | | |
|---|---|---|---|---|---|---|
| 2 | 7681**** | Juan Montes | **20-25** | Marketing | **20.000-30.000** | Gastritis. |

**Codificación por arriba y por abajo:** Consiste en ampliar el rango, para que sea difícil identificar los valores numéricos que sobresalen y pueden ser destacables y por ende más fáciles de identificar.

| | | | | | | |
|---|---|---|---|---|---|---|
| 5 | 30147735M | Elena Jiménez | 51 | Medicina | **Superior a 20.000** | Ulcera Estomacal. |

Estos métodos que consisten en la reducción de los datos pueden tener alguna desventaja: si el atacante que quiere reidentificar los datos personales tiene información previa o si la reducción de los datos personales ha significado perdida de datos podrían ser algunos ejemplos claros.

**Método de introducción de perturbaciones.**

Al contrario que el método mostrado anteriormente, este método persigue introducir nuevos datos para cambiar los datos personales, dificultando la reidentificación de los mismos, aunque un atacante accediese a los datos no podría estar a ciencia cierta seguro de cuáles son los datos originales. Dentro de este método tenemos tres opciones a identificar.

**Reordenación aleatoria de los datos:** Consiste en variar un dato y reubicarlo en otra parte, creando confusión e impidiendo conocer ese dato real.

| | | | | | | |
|---|---|---|---|---|---|---|
| 1 | 74715300H | Claudia Pérez | 57 | CEO | **21.000** | Gripe |
| 2 | 76819745C | Juan Montes | 22 | Marketing | **100.000** | Gastritis. |

**Sustitución:** Este método consiste en sustituir datos originales por ficticios en un campo determinado, de tal forma que, si se utilizasen estos datos con fines estadísticos, no se perderían propiedades.

| | | | | | | |
|---|---|---|---|---|---|---|
| 1 | ~~**74715300H**~~ | ~~**Claudia Pérez**~~ | 57 | CEO | 100.000 | Gripe |
| 1 | **23796824M** | **Esther Sánchez** | 57 | CEO | 100.000 | Gripe |

**Medias Estadísticas:**

En los campos numéricos, podemos aplicar este método también, se trata en sustituir valores específicos por la media del campo entero. Se podría hacer en este ejemplo con la edad o con el salario. En este caso 44.000 € es el salario medio de todos los valores del campo.

| | | | | | | |
|---|---|---|---|---|---|---|
| 5 | 30147735M | Elena Jiménez | 51 | Medicina | **44.000** | Ulcera Estomacal. |

Estos ejemplos son algunos a fin de entender que significa anonimizar, pero hay muchos más métodos, como: Algoritmo de Hash, algoritmos de cifrado, l-Diversidad, k-Anonimización...

La posibilidad de reidentificar los datos personales es un hecho real, los riesgos[39] más grandes existentes son la **singularización,** consiste en extraer de un conjunto de datos algunos registros que identifican a una persona. La **vinculabilidad** la cual consiste en vincular mínimo dos registros de una persona o grupo de personas, de una base o de varias bases de datos. El último riesgo es la **Inferencia** que es la posibilidad de averiguar con probabilidad significativa el valor de un atributo a partir de los valores de un conjunto de atributos.

Con diferentes riesgos inherentes como en cualquier proceso de seguridad, el proceso de anonimización a elegir es opcional ya que la normativa no especifica cual se debe realizar, hay libertad de elección. Por tanto, cada responsable o encargado del tratamiento deberá decidir qué

[39] La anonimización de los datos personales. Confilegal. Disponible en: https://confilegal.com/20150512-anonimizacion-los-datos-personales-12052015-1850/. Referencia: 15 de diciembre de 2018.

proceso elegir en el abanico de posibilidades que existen. La anonimización debe ser un proceso irreversible, por tanto, hay que tener en cuenta los nuevos métodos que aparezcan para mejorar este proceso e intentar volverlo lo más seguro posible.

# IX. Normativa vs Anonimización.

Como se ha podido observar, no hay ningún método perfecto, pero la normativa intenta paliar su déficit frente a la tecnología, adecuándose a los tiempos modernos, en este caso, su respuesta es el RGPD.

Parece ser que la anonimización y seudonimización podrían ser la solución para el tratamiento de datos personales, pero existe el riesgo de la reidentificación, como ha ocurrido en algunos casos sonados, el caso en 2006 de AOL[40], donde hizo públicas antiguas búsquedas de internet para que investigadores analizasen estos datos y sacasen conclusiones imprevistas utilizando el Big Data, pero este tratamiento de más de veinte millones de búsquedas hechas por más de seiscientos mil usuarios durante varios meses demostró que incluso borrando el nombre de usuario y dirección IP como técnica de anonimización no fue suficiente.

El método utilizado no fue infalible, los usuarios utilizaron estos datos y correlacionando las búsquedas de una misma persona anónima con datos públicos, se llegó a identificar al cliente anónimo (N.º. 4417749), con una señora de Georgia, viuda, de sesenta y dos años. El escándalo fue muy sonado en Estados Unidos, lo cual demostró que ante la cantidad de información de la que se dispone gracias a la red, se pueden cruzar datos (vinculabilidad) incluso habiéndolos anonimizado o seudonimizado y conseguir discernir algunas veces una reidentificación total de la persona en cuestión.

La evolución de la tecnología y la cantidad de datos volcados en la red crea enormes riesgos para la privacidad, algunos métodos utilizados son ineficaces, las medidas preventivas anteriormente para proteger la intimidad eran métodos más sencillos, hoy en día incluso datos no personales podrían conducir a enlazarse con datos personales de manera sencilla y asociarse

[40] A Face Is Exposed for AOL Searcher No. 4417749. NYTimes. Disponible en: https://www.nytimes.com/2006/08/09/technology/09aol.html. Referencia: 12 de febrero de 2019.

a nuestra persona. Esto incide principalmente en el concepto de que es considerado un dato personal, ya que los datos asociados a los personales, como pudieran ser identificadores indirectos son también motivo de discusión, la anonimización es un proceso por el cual se anonimizan los datos personales, pero conociendo los datos no personales, podría ser fácil reidentificar a las personas, o correlacionando los datos con bases publicas donde aparezcan estos identificadores indirectos.

La anonimización quizás es una solución parcial al problema, pero no es un método infalible ni mucho menos, siempre que existan datos que se puedan relacionar datos no personales con los personales.

La sobre protección de las personas a veces conlleva a violar su intimidad, tenemos que hacer valer la minimización para tener los menos datos posibles de los usuarios, no vale resignarse ante la imposibilidad de proteger un derecho que poseen todos los ciudadanos de manera inviolable, pero quizás se deban buscar soluciones nuevas ante un problema que, si no es de actualidad, lo será con el tiempo. La obra de George Orwell, 1984[41]donde se habla de un gran ojo que nos vigila no es ciencia ficción en nuestro presente. Actualmente, se vive conectado continuamente a los Smartphones, tablets, Smart TVs… y ellos a su vez, conectados a internet, la utopía de que se controle a la sociedad a raíz de estos dispositivos es meramente ficción, pero quizás la sociedad debería pararse a pensar que la intimidad es valiosa y que vivir desconectados no es tan negativo como parece.

Hoy en día la única manera de que la privacidad no se pierda, equivale a que nadie conozca determinados datos y nunca sean recabados o a la anonimización por defecto, el problema viene cuando la anonimización por sí misma no puede solucionar y dar respuesta a todos los problemas intrínsecos de la utilización del Big Data, cuantos más datos hay en la red, más tecnología se desarrolla y mejor es la velocidad de procesamiento, lo que conllevara a una situación donde la reidentificación será más rápida y por tanto la anonimización podría fallar más veces.

[41] ORWELL, G. (1949).

La normativa en protección de datos ahonda en la prevención utilizando la seguridad del tratamiento desde el diseño y por defecto, lo cual es un claro beneficio para los interesados, la duda es si en el futuro esto será suficiente, quizás, nos encontraremos como sociedad en un futuro ante la imposibilidad de tratar determinados datos sin una anonimización directa, es decir, creando *nicknames* o nombres virtuales para todos nosotros los cuales sean incapaces de relacionarse con nuestra persona, actualmente es muy común en la red, como, por ejemplo, en el caso de la red social Twitter.

El problema radica en que siempre se podrá volver a reidentificar a una persona enlazando determinados parámetros, por tanto, volvemos al problema de que la anonimización puede que nunca sea perfecta. La normativa europea está en consonancia con la privacidad, lo cual es un paso adelante, como es inevitable hoy en día parar el tratamiento de datos personales, se tendrán que poner las medidas adecuadas para frenar los probables abusos, abogar por una seudonimización estructurada en cualquier tratamiento podría ser una solución, para poder evitar la correlación de datos personales y no personales, pero los costos de una seudonimización en todo tratamiento serian incontables para las empresas. Como solución serviría parcialmente, así cuando se intentasen conectar determinados datos, serían los datos entre dos personas anónimas, aunque fuesen la misma, lo cual podría crear un laberinto. Pero esto es muy difícil de lograr por las medidas que conllevarían tomar para muchas empresas que no tienen los recursos adecuados, y porque, al fin y al cabo, con la cantidad de información pública que dispone la red sobre las personas, siempre existe una conexión con el medio, aunque en vez de conectar Carlos R. y Anónimo 30208492. Conectásemos Anónimo 30208492 y XCQQSC282.

No queda otra que confiar en que la anonimización sea una solución por ahora, ya que la normativa no puede ser cumplida tal y como se encuentra ahora mismo para una cantidad ingente de finalidades de tratamiento para lo cual el Big Data esta creado.

Por ahora existe un ejemplo de utilización de esta tecnología con datos seudoanonimizados, en el cual es beneficiosa, como son los datos de salud, la utilización de datos masivos para correlacionar enfermedades, patologías y síntomas conlleva a una lucha más eficaz conjunta de toda la sociedad médica, compartiendo datos útiles para estudios, utilizando el Big Data de una forma responsable todo son bondades.

Hay un conflicto entre el tratamiento de datos personales seudonimizados con un beneficio evidente para la sociedad, y la posibilidad de que con un estudio profundo puedan ser identificadas personas con patologías severas. La prohibición de utilizar estos datos sería un perjuicio para la sociedad, entre el beneficio de toda la sociedad y el riesgo de determinadas personas la elección es difícil.

Una salida a este entramado seria la prohibición de tratar datos anonimizados siempre que existiera un riesgo a poder relacionar estos datos con fuentes públicas y discernir los datos reales, pero la vasta base de datos existente en la red hace imposible de analizar cada vez que ocurra un caso de anonimización y procesado de datos. Por ahora se debe confiar en que la tecnología avance también en la privacidad y se creen mejores métodos de anonimización, los respectivos a tratamientos de datos personales e incluso algunos que podrían relacionarse con estos.

Partiendo de la idoneidad de realizar una seudonimización en el futuro como método radical de intentar proteger bases de datos y la posible vinculación con datos anonimizados, hay un factor importante entre la normativa que puede ser obviado en este momento.

Según el dictamen del Grupo de trabajo del artículo 29, anonimizar es un tratamiento de datos personales:

*"La anonimización puede ser el resultado de un tratamiento de datos personales realizado para impedir de forma irreversible la identificación del interesado".*[42]

Este concepto de que anonimizar en sí mismo es un tratamiento de datos personales, se ve reforzado en un informe de la AEPD, del siguiente extracto *"En definitiva, de lo establecido en el Reglamento General de protección de datos se desprende que, en cuanto el mismo resulte de aplicación y al menos desde que éste entre en vigor, tanto la anonimización como la*

[42] Dictamen 05/2014. GT29. CE. (técnicas de anonimización.). Disponible en: https://studylib.es/doc/5271173/dictamen-05-2014-sobre-t%C3%A9cnicas-de-anonimizaci%C3%B3n Referencia: 10 de marzo de 2019.

*seudonimización de los datos personales llevarán aparejada la existencia de dos tratamientos sucesivos:* ***el que supone la propia anonimización*** *o seudonimización a partir de los datos personales de que dispone el responsable* ***y el que se lleve a cabo posteriormente con los datos ya anonimizados*** *o seudonimizados."*[43]

Este supuesto parece no ser previsto en la mayoría de las políticas de privacidad de las empresas, ya que muchas veces el aviso de la anonimización de los datos personales es casi residual, la mayoría de las empresas se escudan en el interés legítimo como base legitimadora para la "mejora" de los servicios, el análisis de datos anonimizados para poder dar un servicio de más calidad. Pero quizás la regulación debería poner un énfasis en este apartado, el tratamiento de datos en entornos de Big Data basándose en el interés legítimo es un riesgo inherente para los interesados suficientemente importante como para no informar o no tener el consentimiento expreso de los usuarios a fin de poder realizar el tratamiento de anonimización de sus datos, una vez realizado este proceso, los datos quedaran fuera de la normativa, pero el paso en sí mismo al ser un tratamiento de datos debería considerarse como un tratamiento de vital importancia, que necesita una base legitimadora a su nivel como el consentimiento expreso.

Hoy en día hay excesiva utilización del interés legítimo por parte de las empresas como hemos visto anteriormente, la RGPD y las leyes nacionales como la LOPDDD, deberían ser más estrictas ante este hecho, ya que en todo el RGPD no se comenta siquiera la palabra "anonimización".

[43] Informe 0195-2017. AEPD. (Interés legítimo, portabilidad y blanqueo). Disponible en: https://www.aepd.es/media/informes/2017-0195-interes-legitimo-portabilidad-y-blanqueo.pdf Referencia: 10 de marzo de 2019.

# X. Conclusiones

Las conclusiones que se pueden sacar en el tratamiento de datos personales en el ámbito del Big Data son diversas, como se ha tratado de explicar, la normativa en protección de datos evoluciono de manera más pausada que el increíble auge de las tecnologías de la información, el Big Data ha sufrido una "explosión" mediática, su utilización es cada vez más demandada y se necesita equilibrar el crecimiento, el valor añadido y todo lo que pueda ofrecer el Big Data con la privacidad por defecto y por diseño instaurada por la normativa del RGPD.

Aquí se tienen varias opciones, se debe considerar que el Big Data necesita un encuadramiento en el mundo de la protección de datos, siempre y cuando no se utilicen datos no personales, el Big Data como tratamiento de datos atmosféricos, de tráfico, de contaminación… No conllevaría, en principio, ningún problema a nivel privacidad de los ciudadanos. Ahora bien, cuando los datos tratados son datos personales se precisará encuadrar este tratamiento de alguna forma legal y con una base sólida.

**Primera. - Consentimiento expreso residual y utópico para Big Data:** Como hemos visto en numerosos ejemplos, la mayoría de las empresas optan por basar el Big Data en materia de marketing en el consentimiento expreso cuando fuese este posible, ya que es una base legitimadora para el tratamiento de datos con una única finalidad. Pero el Big Data entendido como el tratamiento de datos en multitud de finalidades variadas, choca frontalmente con esta base legitimadora que su premisa principal es un consentimiento expreso, demostrable, informado y para cada uno de los tratamientos. Por tanto, un Big Data utilizado únicamente en una base de datos para el marketing podría basarse en el consentimiento expreso, pero solo para este tratamiento de datos.

**Segunda. - Abuso de Interés Legítimo como base legitimadora en Big Data:** El problema entre el consentimiento expreso y esta nueva tecnología de múltiples finalidades es que no son compatibles más que para una única finalidad, por la cantidad de finalidades diferentes que tiene el Big Data.

Entonces se ha buscado otra base legitimadora, el supuesto es fácil de predecir, un usuario cede sus datos personales para una finalidad, y con el paso del tiempo, cruzando datos personales

utilizados con una finalidad X buscamos una nueva finalidad para buscar un beneficio añadido. La base legitimadora del consentimiento no habría servido en este caso al cambiar las reglas del juego, nos encontramos en una situación de no retorno en la lucha entre la innovación tecnológica y la protección de datos.

La ley obliga a proteger la protección de datos de las personas del uso de la informática, o lo que es lo mismo, en nuestro caso del Big Data. La nueva normativa hace un claro hincapié en el derecho de informar, siguiendo las bases asentadas en la protección de datos desde el diseño y por defecto, pero no es muy compatible basarse en el consentimiento para estos tratamientos, la mayoría de las personas siendo sinceros no leen las cláusulas de protección de datos, se busca simpleza, rapidez y servicio inmediato, considerando las implicaciones a la privacidad que puedan derivarse de un tratamiento de datos en Big Data donde se busca el beneficio al cruzar cantidades masivas de datos, esto conlleva un riesgo evidente para la privacidad de las personas, incluso con datos seudonimizados, al haber una correlación de datos, las personas podrán ser reidentificadas. es decir, no se vislumbra un futuro al Big Data con la legislación actual siempre y cuando quieran tratar datos personales de los usuarios basándose en el consentimiento.

En cambio, las empresas se basan en el interés legítimo mayoritariamente o en el contrato para dar un servicio de mejor calidad, y con esta responsabilidad de ofrecer un mejor servicio, recabar los datos para hacer tratamientos de Big Data para modernizar sus sistemas y su calidad. Las políticas de privacidad de las empresas intentan eludir las responsabilidades, explicando que se basan en el interés legítimo, en el contrato y en los datos voluntarios que las personas añaden a sus *websites*, como pudieran ser en el caso de Amazon o Airbnb con sus "listas de deseos" o "comentarios de *feedback"*.

Desde la perspectiva proteccionista, se entiende que estas prácticas deberían informar de una manera mucho más específica, de los riesgos inherentes del Big Data, permitir que todos estos datos sean tratados para estas prácticas son una amenaza para la intimidad de los interesados, un riesgo del cual no son tan conscientes como deberían.

**Tercera. - Anonimizar propiamente es un tratamiento de datos personales y debería realizarse con consentimiento expreso:** La opción de anonimizar que utilizan la mayoría de

las empresas debería ser informada de una manera mucho más clara, basándonos en el informe[44]de la AEPD y en el dictamen[45] del GT29 de la comisión europea, la anonimización es en sí misma es un tratamiento de datos personales, si las empresas se basan en el consentimiento expreso, necesitarán un consentimiento para este tratamiento de datos, si se basasen en otra base legitimadora como un contrato o interés legítimo, deberían informar, no con un aviso casi oculto en la política de privacidad basándose en el tratamiento de datos con fines estadísticos. Si no, con un aviso más claro y en muchos casos debería darse el consentimiento expreso para anonimizar los datos personales. Se entiende que dar el consentimiento expreso para una simple finalidad es legítimo, por tanto, sin ninguna referencia específica a la anonimización en toda la normativa, quizás debería hacerse hincapié en que anonimizar debería aparejar el consentimiento expreso, a fin, de evitar posibles re-identificaciones futuras con sorpresas para los interesados que pueden aludir a que desconocían dichos tratamientos. Realizar tratamientos de datos anonimizados esta fuera de la normativa, pero convertir estos datos en anónimos conlleva un paso muy importante, conlleva que la persona que cede sus datos dejara de poseer la potestad para decidir sobre ellos y debería ser solo y únicamente con su consentimiento expreso con la información relevante de las consecuencias de una posible reidentificación en el caso de tratamientos de Big Data, como en el caso de AOL que vimos anteriormente.

**Cuarta. – el Big Data sufre un crecimiento anual y la anonimización es una solución real al conflicto:** En el caso de buscar la solución definitiva al Big Data, la anonimización puede ser la solución, de esta forma el tratamiento quedaría fuera de la normativa y podrían utilizarse estos datos en el entorno del Big Data sin preocupaciones (siempre y cuando se utilicen métodos seguros que no permitan la reidentificación).

La evolución del internet de las cosas, la recogida de datos por diferentes dispositivos ya no puede ser frenada, es el futuro y presente, tenemos que buscar la protección jurídica de los individuos, y encontrar el equilibrio entre su privacidad y los beneficios que puedan sacar grandes empresas del tratamiento de datos, siempre defendiendo a los individuos como dicta la Constitución. Por esta razón, lo ideal sería evitar el tratamiento de datos personales en la medida de lo posible, si fuera posible utilizar los métodos de anonimización o seudonimización basados

[44] Ídem.

[45] Dictamen 05/2014. GT29. CE. (técnicas de anonimización). https://studylib.es/doc/5271173/dictamen-05-2014-sobre-t%C3%A9cnicas-de-anonimizaci%C3%B3n Referencia: 10 de marzo de 2019.

en el consentimiento expreso, la información a los ciudadanos debe ser lo más clara y resumida posible, sería positivo utilizar modelos por capas e implantar una seudonimización y anonimización casi por defecto, aunque esto es utópico en muchas empresas por los costos que conllevaría, pero no deja de ser un marco ideal a soñar para el futuro.

La importancia puede radicar en el comienzo de todo el proceso, es un gran avance que el RGPD se base en la privacidad por defecto y por diseño, los procedimientos iniciales al recabar los datos personales pueden hacerse de una manera correcta y respetuosa con la privacidad, solo debemos conocer los métodos y aplicarlos desde el comienzo, aunque posteriormente los datos se anonimicen, saliéndose de la normativa del RGPD y LOPDGDD.

Las autoridades de control deben ser activas en aplicar guías para el tratamiento en diferentes sectores y penalizar las malas prácticas en perjuicio de las irregularidades, la normativa les da la potestad de aplicar fuertes sanciones a las empresas que caigan en el incumplimiento, de hasta 20.000.000 € o el 4% de la facturación, buscar el beneficio de los interesados debería ser la prioridad, no se debe permitir que la privacidad sea un elemento olvidado, hay que proteger este derecho fundamental. La oportunidad de poder anonimizar los datos es la vía de escape a un tratamiento en Big Data respetuoso con la privacidad y la solución más sensata y factible para cumplir en materia de Compliance y protección de datos.

Es contradictorio que hoy en día con las redes sociales, las personas expongan su vida privada sin ningún miramiento, no se valora este derecho fundamental, quizás se deba este hecho a una falta de educación en este aspecto por parte del estado, puede que haga falta un programa de enseñanza para la población respecto a la importancia de mantener la intimidad personal en el entorno personal.

Que los ciudadanos hagan su vida pública en cada instante. No debería impedir que la ley regule y proteja este derecho fundamental que tenemos todos, por tanto, el camino está marcado, el Big Data debe evolucionar a la par que la normativa, y si el proceso no puede darse, la anonimización es la solución, siempre y cuando sea efectiva y actualizando sus métodos con las nuevas tecnologías para poder impedir que los datos sufran un proceso de reidentificación, aunque como hemos visto, no existe un método infalible.

**Quinta. - Incluso la anonimización no libera de todos los riesgos:** El Big Data supone una amenaza a la privacidad basándonos en su naturaleza de cruzar datos, en el futuro podríamos encontrarnos con que el análisis de los datos pueda adelantarse a decisiones futuras de las personas, esto querrá decir juzgar con predicciones cada vez más precisas las futuras decisiones dándolas como predichas. Este sería un ataque a la libertad y libre albedrío de las personas. En Amazon o Netflix este método ya se utiliza para predecir nuestros gustos, pero quien sabe, si en el futuro, estos análisis son utilizados para otros fines, cómo, conocer nuestra predisposición genética a determinadas enfermedades y el consiguiente riesgo para una aseguradora de vida adjudicar un seguro.

Cada vez se recaban más datos y a veces deberíamos preguntarnos si son realmente necesarios, el ejemplo más claro es el servicio de un Taxi, en el cual no hace falta identificarnos, en contra con un ejemplo como Uber, la empresa conoce perfectamente quien somos, a donde vamos, nuestros trayectos, donde vivimos… Está claro que los beneficios en seguridad son notables, al controlar el trayecto y con qué conductor se realiza el viaje, podrá ser más sencillo poner una reclamación, encontrar un objeto perdido o proteger al usuario ante farsantes (taxis falsos).

El riesgo de la vinculabilidad ante filtraciones de información es una realidad, el Estado mismo hace públicos datos abiertos que pueden enlazarse con factores indirectos de alguna u otra forma, lo cual puede conllevar sin querer a apoyar métodos de reidentificación que ataquen la privacidad de las personas. Los ciudadanos deben abogar por una "privacidad desde la responsabilidad" [46] siendo conscientes de que comparten, cómo y cuándo. Y las implicaciones de sus actos, indirectamente. En consecuencia, se considera vital un conocimiento mayor en qué es la privacidad, cómo proteger está y valerse más del consentimiento expreso que de otras bases como el interés legítimo para tratamientos de datos anonimizados.

**Sexta. - Modelo Sanitario de Big Data buen ejemplo de lo que debe hacerse:** El ejemplo que seguir, es el del mundo sanitario, cumpliendo con el RGPD y la protección de datos desde el diseño y por defecto, seudonimiza los datos personales en busca de un beneficio para la sociedad desde el comienzo. Un mundo anónimo es sinónimo de un Big Data con privacidad.

[46] MAYER-SCHÖNBERGER – KENNETH CUKIER. (2013).

# XI. Bibliografía y Legislación Citada.

## XI.1. Bibliografía.


- AIRBNB. (2019), "Política de privacidad de Airbnb". (Disponible en: https://www.airbnb.es/terms/privacy_policy.). Fecha de última consulta: 8-03-2019.

- ACED, E-HERAS,MªR-SÁIZ,C.A (Coordinadores)- ÁLAMO,JMª-ARMENTIA,P-BRITO,N-BUEZO,L-COLOM,JL-CORDÓN,C-CORREDERA,R-DIAZ,M-DIAZ,P-FERNANDEZ,C-GARCÍA,D-GONZÁLEZ,F-GRIFOLL,L.E-LAREDO,J-MARTÍN,Y.D-MONLEÓN,J.R-MORA,E-MUÑOEZ,A-ORTIZ,P-PANTOJA,M.A-PELEGRIN,I-PÉREZ,D-SANCHEZ,O-SARACIBAR,E-TORRERO,J.A (2018) *Código de buenas prácticas en Protección de Datos para proyectos de BIG* DATA,AEPD, Pág. 8.

- AEPD. (2016), "Orientaciones y garantías en los procedimientos de anonimización de datos personales.", Guía, Págs. 11-14. (Disponible en https://www.aepd.es/media/guias/guia-orientaciones-procedimientos-anonimizacion.pdf). Fecha de última consulta: 10-12-2018.

- BARBARO, M – ZELLER, TOM. (2006), "A Face Is Exposed for AOL Searcher No. 4417749". NYTIMES. (Disponible en https://www.nytimes.com/2006/08/09/technology/09aol.html). Fecha de última consulta: 26-02-2019.

- ELIXIR, (2018), "*Who we are*". (Disponible en: https://www.elixir-europe.org/about-us/who-we-are.). Fecha de última consulta: 8-03-2019.

- EUROPEAN PLATFORM ON RARE DISEASE REGISTRATION, (2018). (Disponible en https://eu-rd-platform.jrc.ec.europa.eu/#.). Fecha de última consulta: 9-03-2019.

- FACUA, (2018), "La AEPD concluye que el Ministerio de Justicia se saltó la Ley de Protección de Datos con LexNet." (Disponible en: https://www.facua.org/es/noticia.php?Id=12662). Fecha de última consulta: 5-03-2019.

- GIL GONZÁLEZ, E. (2015). *Big Data, Privacidad y Protección de Datos*, 1º edición, Madrid, AEPD, Página 129.

- HORIZONTE 2020, (2015), "¿Qué es Horizonte 2020?" (Disponible en https://eshorizonte2020.es/que-es-horizonte-2020). Fecha de última consulta: 8-03-2019.

- GARRALÓN, P. (2015). "La anonimización de los datos personales.". CONFILEGAL, pág. 1-5. (Disponible en https://confilegal.com/20150512-anonimizacion-los-datos-personales-12052015-1850/). Fecha de última consulta: 15-12-2018.

- MANDADO PÉREZ, E- FERNÁNDEZ SILVA – CELSO, MARCOS ACEVEDO, J-ARMESTO QUIROGA, J- RIVAS LÓPEZ, JL-NÚÑEZ ORTUÑO, JMª (2018) "Tecnicismos, neologismos y extranjerismos en español" *RAE*,7, pág. 11. (Disponible en http://revistas.rae.es/bilrae/article/view/218/524). Fecha de última consulta: 20-11-2018.

- MARR, B. (2016), *Big Data in Practice: How 45 Successful Companies Used Big Data analytics to deliver extraordinary*, John Wiley & Sons Inc, Págs. 163-167. 223-228.

- MARR, B. (2018), *Data Strategy: Como beneficiarse de un mundo de Big Data, Analytics e Internet de las cosas*, 1ª edición, Teell Editorial, S.L, Págs. 24-27.

- MAYER-SCHÖNBERGER, V. – CUKIER, K. (2013) *Big Data. A Revolution That Will Transform How We Live, Work, and Think.*, 4º edición, Nueva York.

- MOVISTAR, (2019), "Política de privacidad de Movistar." (Disponible en http://www.movistar.es/particulares/centro-de-privacidad/). Fecha de última consulta: 7-3-2019.

- ORWELL, G. (1949). *1984*. Londres. Delbolsillo.

- UNIVERSITAT POMPEU FABRA, (2015), "ELIXIR acelera con financiación del programa europeo Horizon 2020". (Disponible en https://www.upf.edu/web/e-noticies/archivo/-/asset_publisher/wEpPxsVRD6Vt/content/id/2669044/maximized#.XIQLeChKhPY.). Fecha de última consulta: 8-03-2019.

## XI.2. Legislación Citada.

- Constitución Española. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-1978-31229 Artículos 18.1 y18.4.

- LOPDGDD. Disponible en: https://www.boe.es/boe/dias/2018/12/06/pdfs/BOE-A-2018-16673.pdf Artículos 6,7,9,9.1,77.3. y Disposición adicional décimo séptima.

- RGPD. Disponible en: https://www.boe.es/doue/2016/119/L00001-00088.pdf Considerandos 6,7,32,38,40,42,43. Y Artículos 4.11,4.5,6,7,9,22,25,83.5.

- **2007.** Dictamen 04/2007. GT29, CE. (Concepto de datos personales).

- **2014.** Dictamen 05/2014. GT29. CE. (técnicas de anonimización).

- **2017.** Informe 0195-2017. AEPD. (Interés legítimo, portabilidad y blanqueo).

# XII. Tablas.