Universidad de Valladolid

Facultad de Derecho

Grado en Derecho

Big data y protección de datos: la apuesta de la Unión Europea

Presentado por:

Beatriz Jimena Tamayo Velasco

Tutelado por:

Luis Velasco San Pedro

Valladolid, 5 de junio de 2020

Resumen

El 25 de mayo de 2018 entró en vigor el Reglamento General de Protección de Datos (Reglamento 2016/679), la más reciente propuesta europea para afrontar los desafíos que el *big data* plantea sobre la privacidad de las personas. Este Trabajo se centrará en su estudio; sus novedades respecto a la derogada Directiva de Protección de Datos (Directiva 95/46/CE), sus provisiones más controvertidas y su pretendida repercusión internacional. En base a este análisis, se desarrollará una propuesta de reforma para abordar los puntos más débiles detectados en dicho instrumento jurídico.

Palabras clave

Big data, privacidad, protección de datos, datos personales, era digital, consentimiento informado, responsabilidad proactiva, RGPD.

Abstract

On 25th May 2018, the General Data Protection Regulation (Regulation 2016/679) -the most recent European proposal to face the challenges placed by *big data* on users´ privacy- came into force. The present Work will focus on its study; its changes compared to the previous Data Protection Directive (Directive 95/46/EC), its most controversial provisions and its pretended international impact. Based on this analysis, a reform proposal will be developed to deal with the weakest spots detected in this legal instrument.

Keywords

Big data, privacy, data protection, personal data, digital era, informed consent, accountability, GDPR.

ÍNDICE

1. INTRODUCCIÓN

Cuando pensábamos que lo habíamos visto todo, el *big data* (o datos masivos) ha traído consigo una auténtica revolución de la era digital que conocíamos hasta ahora. El liderazgo económico no se determina ya tanto por la posesión del petróleo u otras materias primas físicas, sino por el control de lo "intangible"; esto es, de los datos.

En la denominada "economía de los datos", las empresas desarrollan estrategias de *marketing* basadas en el uso de los datos, diseñan nuevos modelos de negocio en el marco de mercados de doble cara y desvirtúan conceptos tan básicos como el precio monetario a pagar por un servicio.

Las posibilidades del *big data* no se limitan al lucro individual, sino que pueden contribuir significativamente al bien común, gracias a su aplicación en el sector científico o en las Administraciones Públicas.

Evidentemente, el *big data* presenta también un lado oscuro cuyo peso es igual o superior al de todas sus bondades. El riesgo más evidente se refiere a la privacidad de los individuos, y esto no es ningún secreto. Escándalos de privacidad como el de *Cambridge Analytica*,[1] entre otros muchos, ponen de manifiesto la realidad de estos peligros y evidencian la insuficiencia de las normas que nos protegían hasta ahora.

Todos estos riesgos se traducen en desafíos para el Derecho, que ha de llenar este vacío jurídico y ofrecer soluciones adentrándose en un campo aún bastante inexplorado. En el ámbito de la privacidad, la respuesta ha de proceder desde el área jurídica de la protección de datos.

Esta problemática ha venido a coincidir con la entrada en vigor, el 25 de mayo de 2018, del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de Protección de Datos; en adelante, "el RGPD" o "el Reglamento"). Aunque el contenido de este Reglamento es de carácter general y más amplio, abarcando todas las cuestiones que tienen que ver con la protección de datos de carácter personal, no hay duda de que los problemas que plantea el *big data* hoy en día deben resolverse en Europa partiendo de sus disposiciones. Por esta razón, se hace necesario estudiar sus grandes orientaciones.

[1] En el apartado 8.2. analizaremos el escándalo de *Cambridge Analytica*.

La UE ha puesto grandes esperanzas en este Reglamento, que parece establecer un sólido y actualizado marco de protección de datos, acorde con su ambicioso plan por superar el desfase que presenta Europa respecto a China y Estados Unidos en su pugna por el liderazgo digital. De hecho, tratándose de un instrumento jurídico pionero, se espera que su eficacia se extienda mucho más allá de sus fronteras.

A pesar de sus escasos dos años de recorrido, ya es el momento de comenzar a evaluar la eficacia de la propuesta europea. El RGPD será nuestro principal objeto de atención, por lo que nos volcaremos en él con un triple objetivo: estudiar su articulado, destacar los puntos de debate más actuales y ,finalmente, plantear un índice de propuestas.

Comenzaremos, pues, con un análisis pormenorizado de las novedades que incorpora el Reglamento en relación con la derogada Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante, "Directiva de Protección de Datos" o "la Directiva").

A continuación, expondremos los puntos que más controversia han levantado desde su entrada en vigor. Daremos, además, unas pinceladas acerca de su pretendido carácter internacional.

Sobre la base de todo lo anterior, podremos desarrollar un pequeño programa de reforma con la intención de reforzar sus flancos débiles para consolidarlo como un verdadero referente en la protección de datos a nivel mundial.

2. CONCEPTO Y CARACTERES DEL BIG DATA

Al oír hablar del *big data,* probablemente se nos vengan a la cabeza conceptos como análisis masivo de información e inteligencia artificial, algoritmos y modelos matemáticos, *machine learning,* políticas de privacidad o *cookies*. Quizá, si prestamos frecuente atención a los medios, también pensemos en los escándalos relacionados con la violación de la privacidad que gigantes empresariales como *Google*, *Amazon* o *Facebook* protagonizan día tras día.

Sabemos que el *big data* es una realidad presente en nuestras vidas de mil y una maneras. No hay más que leer los titulares de los periódicos o ver el Telediario un día cualquiera para comprender hasta qué punto es cierta esta afirmación. Esta relevancia práctica se evidencia

incluso con más fuerza en situaciones extraordinarias, como es la crisis sanitaria global en la que nos encontramos.[2]

Sin embargo, ¿Cuántos pueden definir concretamente qué es el *big data*?

Para ponernos en contexto, hemos de imaginar inmensurables cantidades de información digital de las que –tras un proceso de análisis y tratamiento basado en el uso de algoritmos- puede extraerse un gran valor económico.

El avance significativo que trae consigo la revolución del *big data* no es el análisis de datos en sí; sino la escala a la que se realiza semejante análisis. Distintos sectores sociales -desde empresas hasta las Administraciones Públicas- han estado siempre interesados en el análisis de la información que proporcionaban ciudadanos o clientes. Prueba de ello son los censos o estadísticas oficiales realizadas por el Estado, o las tarjetas de fidelización y encuestas tan comunes en los comercios de toda la vida.

Sin embargo, la capacidad de recoger, almacenar y procesar inmensas cantidades de información es algo que debemos a las nuevas tecnologías. Surgen así otras utilidades y posibilidades de los datos; con los consecuentes nuevos riesgos y peligros que ello comporta.

A pesar de que no existe una manera única e infalible de precisar el término, cualquier definición debería tener en consideración cuatro factores, las "cuatro v" de los datos masivos: volumen, variedad, valor y velocidad de procesamiento.[3]

En la denominada era digital en la que nos encontramos, cualquier actividad que desarrollemos en la red deja un valioso rastro, aun sin nosotros saberlo. Dicho de otro modo, nuestra actividad en Internet genera una ingente cantidad de información, que puede ser utilizada de manera provechosa por aquellas empresas dedicadas al análisis masivo de datos. Cuando compramos un libro por *Amazon*, publicamos una foto en *Instagram*, damos un *like* en *Facebook* o realizamos una búsqueda en *Google*, estamos compartiendo una serie de información acerca de nuestra persona. Los datos que manejan dichas empresas proceden de esa información que voluntariamente compartimos (por ejemplo, a través de las redes sociales), información cosechada de otras formas (por ejemplo, a través de las *cookies*) o información inferida a través del análisis de otros datos.

---

[2] Dado el extraordinario carácter de esta situación, en el Apéndice estudiaremos la relación existente entre *big data* y COVID-19.

[3] HERRERO SUÁREZ, Carmen. "La economía de los grandes datos o Big Data desde el Derecho de la competencia: ¿nuevos problemas? ¿nuevas soluciones?". *Revista de Derecho de la Competencia y de la Distribución,* núm. 23, 2018, p. 3.

La incesante expansión de la economía digital y sus diversas manifestaciones (redes sociales, buscadores de Internet, servicios de compraventa online, el fenómeno del *Internet of Things,* etc) ha dado lugar a un crecimiento exponencial de la cantidad de datos disponibles al servicio de sus operadores. Por poner algunas cifras, 24 petabytes de datos eran procesados al día por *Google*, más de 10 millones de fotos se subían cada hora a *Facebook* y se publicaban más de 400 millones de *tweets* en *Twitter* diariamente ya en el año 2012.[5]

No es difícil observar que la posibilidad de obtención y almacenamiento de semejante cantidad de información se debe a la digitalización de la economía. De hecho, en 2013, menos del 2% de la información procedía de fuentes físicas.[6] En épocas anteriores, el proceso de recolección sería tan costoso y el almacenamiento tan complicado, que sería impensable acumular tales cantidades de información.

A esto nos referimos cuando hablamos del volumen y la variedad de la información como dos de los rasgos fundamentales de los datos masivos.

Por otro lado, los datos masivos carecerían de relevancia práctica si no se hubiesen desarrollado paralelamente técnicas de análisis y procesamiento de datos que redujesen significativamente los tiempos necesarios para obtener conclusiones útiles de los mismos. Estos procesos se realizan a través de aplicaciones analíticas y algoritmos que pueden llegar a analizar la información incluso a tiempo real.

Hablamos del tercer factor imprescindible de los datos masivos, la velocidad de procesamiento. Este factor cobra aún mayor relevancia si tenemos en cuenta la rapidez con la que la información que proporcionamos a los operadores de la economía digital queda obsoleta o desfasada.

Podemos ilustrar este hecho con el fenómeno del *Internet of Things*, que permite la interconexión de aparatos entre sí a través de las redes sin necesidad de intervención humana.[7] Por ejemplo, nuestro teléfono móvil podría estar interconectado a cualquier electrodoméstico de nuestra casa e informar continuamente del estado en el que se encuentre.

---

[5] MAYER-SCHÖNBERGER, Viktor y CUKIER, Kenneth. *Big Data: la revolución de los datos masivos*. Turner Noema, 2013, p. 19.

[6] Ibid, p. 20.

[7] Deloitte. "IoT-Internet of Things". (*Deloitte*, s.f.). Disponible en <https://www2.deloitte.com/es/es/pages/technology/articles/IoT-internet-of-things.html> [Consulta: 10-02-2020].

La información que se proporciona a través de este sistema se actualiza continuamente, por lo que queda desfasada con igual velocidad.

El último ingrediente esencial del *big data* es el valor económico asociado a los datos. Es precisamente este el que justifica los esfuerzos que ponen las empresas en desarrollar mejores y más eficientes técnicas de recolección, análisis y procesamiento de datos.

Básicamente, las empresas obtienen utilidad del *big data* través de dos vías.

En primer lugar, pueden aprovecharse de las conclusiones extraídas del análisis de los datos para predecir el comportamiento de los consumidores en el futuro y facilitar la toma de decisiones relevantes. De esta forma, las empresas pueden ofrecer una publicidad más personalizada, en función de las particularidades y gustos del cliente; desarrollar productos mejor adaptados a la demanda, o diseñar políticas personalizadas de precios. Según un estudio de la OCDE en 2015, las empresas que aplican estrategias de *data-driven innovation* podrían experimentar un crecimiento del 5% al 10%, respecto a aquellas que no utilizan tales tecnologías.[8]

En segundo lugar, no podemos olvidarnos de aquellas empresas que han implantado un modelo de negocios que gira en torno al valor económico de los datos; es decir, cuya principal fuente de ingresos procede de la venta de datos a terceros. Este modelo de negocios se integra en el marco de los denominados mercados de doble cara (*multi-sided* o *two-sided markets*). Un mercado es de doble cara cuando reúne tres requisitos:[9]

- Hay dos demandas diferenciadas, aunque interdependientes entre sí.
- El valor obtenido por uno de los lados de la demanda incrementa a medida que aumenta el número de consumidores de la otra vertiente.
- La existencia de una empresa intermediaria o "plataforma" es necesaria para internalizar las externalidades generadas por uno de los lados de la demanda.

La estrategia de precios adoptada en estos mercados difiere de aquella utilizada en cualquier otro mercado, considerando que los datos son el activo más preciado de las empresas "plataforma" y el hecho de que el valor que obtiene uno de los lados de la demanda se determina en función al tamaño del otro lado. Con el objetivo de recabar la mayor cantidad

[8] BOURREAU, Marc; DE STREEL, Alexandre y GRAEF, Inge. "Big Data and Competition Policy: market power, personalised pricing and advertising". *Centre on Regulation in Europe,* 2017, p. 14.

[9] EVANS, David. "The antitrust economics of two-sided markets". *American Enterprise Institute*, 2002, p. 43. Disponible en <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=332022>, [Consulta: 11/02/2020].

de datos posible, la empresa "plataforma" puede ofrecer servicios a coste 0 a uno de los lados de la demanda (el más afectado por el precio), cargando con los costes al otro lado de la demanda (el que más valora el tamaño de la otra vertiente).

El mejor y más claro representante de esta estrategia es *Google*, que ofrece servicios aparentemente "gratuitos" como buscador de Internet a todos sus usuarios. Estos servicios "gratuitos" son subsidiados por el otro lado de la demanda, constituido por aquellas empresas que desean obtener los datos y hacer llegar su contenido publicitario al mayor número de usuarios posible. En realidad, estamos ante una nueva modalidad de pago: los usuarios de *Google* no están obteniendo los servicios del buscador de Internet gratuitamente, sino que pagan con sus datos.[10]

3. BENEFICIOS Y RIESGOS

Las empresas privadas pueden ser las grandes beneficiarias de la aplicación de estrategias basadas en *big data* a sus modelos de negocio; aunque no las únicas. Administraciones Públicas, consumidores individualmente considerados y la sociedad en su conjunto también experimentan ventajas gracias a su utilización.

Son múltiples los ejemplos que demuestran cómo el *big data* puede contribuir significativamente a mejorar el bienestar social. Las posibilidades de los datos masivos son muchas en el campo de la sanidad pública. En el campo de la genómica, la capacidad de analizar y procesar con rapidez grandes bases de datos de pacientes facilita la detección del cáncer y enfermedades o la predisposición hacia ciertas enfermedades hereditarias, mejorando su diagnóstico y anticipando su tratamiento.

Por otro lado, el análisis de *big data* puede contribuir a frenar la propagación de enfermedades contagiosas, como sucedió en 2009 en relación a el virus H1N1, un nuevo virus de la gripe que en aquel momento generó un gran revuelo. El virus se expandía a tan alta velocidad que los organismos de sanidad pública pudieran reaccionar con suficiente prontitud. En este escenario, *Google* se coronó como un predictor mucho más eficiente de la propagación de dicha enfermedad.[11] Partiendo de los millones de búsquedas que se realizan a diario en su buscador, *Google* se centró en identificar a los enfermos a través de sus

[10] BUDZINSKI, Oliver y STÖHR, Annika. "Competition policy reform in Europe and Germany – institutional change in the light of digitization" *European Competition Journal*, vol. 15, núm. 1, 2019, p. 23.

[11] MAYER-SCHÖNBERGER, *Big Data: la revolución…,* cit., p. 11.

búsquedas en Internet. A partir del análisis de dichas búsquedas, *Google* fue capaz de predecir con mayor exactitud y prontitud que las estadísticas oficiales la propagación de la enfermedad.

Hemos adelantado ya cómo la reciente pandemia mundial ha vuelto a demostrar la interacción entre sanidad pública y *big data*. Las interacciones del *big data* con el COVID-19 son múltiples y pueden observarse en diferentes ópticas, desde la predicción de la existencia de la pandemia hasta la gestión de la sanidad pública en la propagación de la enfermedad. Dado su actual impacto social, estudiaremos esta relación más adelante en mayor profundidad.[12]

Las Administraciones Públicas también aplican *big data* en otras áreas de actuación. Sin ir más lejos, el Instituto Nacional de Estadística (INE) rastreó los movimientos de los teléfonos móviles en España entre los días 18 al 21 de noviembre del pasado 2019.[13] Para realizar este experimento, las tres grandes operadoras móviles españolas (*Movistar, Vodafone* y *Orange*) aportaron al INE los datos agregados de sus usuarios, manteniendo así la anonimidad de los sujetos.[14] El objetivo del rastreo era obtener información relevante acerca de los desplazamientos diarios y de fin de semana de los españoles, conocer a qué lugares se dirigen para pasar sus vacaciones o identificar los denominados "municipios dormitorio". Esta información puede ser usada por el gobierno español para mejorar y modernizar la infraestructura y sistema de transportes públicos, modificar la distribución de servicios públicos de acuerdo a los ciudadanos o emprender iniciativas de revitalización de determinados territorios.

Asimismo, la Consejería de Turismo de Andalucía ha desarrollado el proyecto SmartData, con la finalidad de mejorar la gestión de servicios turísticos.[15] El proyecto, basado en el análisis de datos obtenidos a través de las más diversas fuentes -desde estadísticas oficiales hasta *likes* en las redes sociales-, proporciona información muy relevante acerca del comportamiento de los turistas y sus elecciones. Así, por ejemplo, se ha llegado a la conclusión de que un turista alemán planifica sus vacaciones con mayor antelación que un

---

[12] Ver Apéndice.

[13] El País. "El INE seguirá la pista de los móviles de toda España durante ocho días". (*El País*, 29-10-2019). Disponible en <https://elpais.com/economia/2019/10/28/actualidad/1572295148_688318.html> [Consulta: 11-2-2020].

[14] Ibid.

[15] El País. "30 millones de datos diarios para conocer al turista". (*El País*, 21-08-2019). Disponible en <https://elpais.com/economia/2019/08/20/actualidad/1566330581_839728.html> [Consulta: 11-2-2020].

turista inglés.[16] Basándose en el lugar de procedencia del turista, esta información puede ayudar a determinar cuál es el mejor momento para lanzar una campaña publicitaria.

En cuanto a los consumidores, las implicaciones del *big data* son ambivalentes para ellos.

Ciertamente, la aplicación del *big data* por parte de las empresas permite a los consumidores recibir una publicidad más acorde a sus gustos y necesidades. De igual manera, dado que las compañías tienen en cuenta las preferencias de sus consumidores a la hora de modificar y mejorar los productos y servicios que ofrecen, los clientes tenderán a obtener mejores productos de acuerdo con su criterio.

Desde otra perspectiva, los mercados de doble cara presentan la característica de que una parte de la demanda pueda adquirir servicios aparentemente de manera gratuita. No debemos olvidar que, aunque el coste monetario sea 0, los clientes están pagando los servicios que obtienen con sus datos. En este área, los consumidores se verán favorecidos en función del valor que asocien a sus datos y de la información que dispongan acerca del uso que las empresas suministradoras hagan de sus datos.[17]

Además, la tenencia de datos de los consumidores puede llevar a la aplicación de políticas de discriminación de precios. El conocimiento de una serie de datos acerca de los clientes puede ayudar a determinar la disposición de este a pagar cierta cantidad de dinero. Si la empresa conoce cuál es la máxima cantidad que su cliente está dispuesto a pagar, puede reducir o incrementar los precios en consecuencia, disminuyendo el beneficio personal obtenido por el cliente e incrementando el de la empresa.

Diferente -aunque directamente relacionado con lo anterior- serían las políticas de discriminación en la búsqueda (*search discrimination*).[18] Las empresas pueden ofrecer distintos productos o servicios a sus clientes, en base a su disponibilidad a pagar. Un estudio demostró en 2012 que una agencia de viajes ofrecía hoteles más caros a aquellos clientes que accedían a sus servicios desde un ordenador *MAC* respecto de aquellos que accedían a través de otro ordenador común.[19]

En definitiva, es difícil concluir en términos genéricos si el *big data* favorece o perjudica al bienestar global de los consumidores.

---

[16] Ibid.

[17] BUDZINSKI, op. cit., pp. 25-29.

[18] BOURREAU, op. cit., p. 41.

[19] Ibid.

No es difícil adivinar que, aparte de todos sus beneficios, el uso de *big data* también implica importantes riesgos. Los riesgos que plantea el *big data* se traducen en nuevos desafíos y retos para el Derecho, que son abordados fundamentalmente desde tres ramas jurídicas: el Derecho del consumo, el Derecho de la protección de datos y el Derecho de la competencia.

Los riesgos más perceptibles son aquellos que se refieren a la privacidad de los usuarios. Sin apenas ser conscientes de ello, las empresas manejan datos que pueden afectar en todas las dimensiones de nuestra vida, desde conseguir un trabajo o una póliza de seguro, hasta conseguir una pareja. De las distintas categorías de datos que pueden proporcionarse a una empresa, el debate gira en torno a los "datos de carácter personal".

Como ya hemos visto, el control sobre estos datos permite a las compañías ejecutar acciones discriminatorias, que son especialmente difíciles de frenar o castigar cuando proceden de la aplicación de algoritmos que toman decisiones de manera automática, sin intervención humana.

Otro riesgo que se plantea tiene que ver con la seguridad de los datos que se hallan en poder de las compañías. ¿Cuántas veces hemos escuchado situaciones en que *hackers* han conseguido introducirse en los sistemas informáticos de grandes empresas y hacerse con las bases de datos que estas poseen? A medida que las tecnologías avanzan, la inseguridad de las bases de datos aumenta.

Un problema a mayores es la anonimización de los datos. Las tecnologías disponibles en la actualidad facilitan la posibilidad de reidentificación de los individuos, con lo que es prácticamente imposible garantizar la existencia de bases de datos completamente anónimas.

La Protección de datos, en mayor medida, y el Derecho del consumo, en menor medida, son las dos áreas jurídicas que tratan de dar solución a tales problemas. En el marco de la Unión Europea, el RGPD abarca estas y otras cuestiones que se plantean en la era digital.

Una segunda (y mucho más imperceptible) categoría de riesgos del *big data* se refiere a los potenciales problemas que surgen para garantizar un nivel adecuado de competencia en los mercados. Este es el área del Derecho de la competencia.

Hasta ahora, las autoridades de la competencia no habían considerado que la posesión de bases de datos por parte de las empresas pudiese hacer peligrar el delicado equilibrio de los mercados.

Parece que, poco a poco, la tendencia comienza a invertirse. En los últimos años, hemos sido testigos de mediáticos procesos cuyo punto de mira está el comportamiento competitivo

de las empresas. En este escenario, se plantean cuestiones aún por resolver: ¿Hasta qué punto debe intervenir el derecho de la competencia en relación a este tipo de sucesos? ¿En qué medida concierne al derecho y las autoridades de la competencia garantizar el derecho de privacidad de los consumidores? ¿Son adecuados los instrumentos del derecho de la competencia para hacer frente a estos potenciales riesgos?

4. EL IMPACTO DEL BIG DATA EN EL DERECHO DE LA UE

En la era digital, las superpotencias luchan por el control de lo "intangible". A pesar de carecer de dimensión física, los datos son uno de los activos más cotizados a día de hoy.

Los datos son uno de los ingredientes claves de la economía digital; la materia prima que -junto con otros ingredientes, como la inteligencia artificial- puede servir de base para la resolución de desafíos que se plantean en la actualidad en todo tipo de ámbitos, públicos y privados, como hemos expuesto anteriormente.

En esta carrera, la Unión Europea se ha visto claramente desbancada por sus dos mayores rivales, Estados Unidos y China. Las cifras son escalofriantes. El 92% de los datos generados a nivel global estarían almacenados en empresas estadounidenses, según reflejan estudios actuales.[21]

Las 5 mayores empresas tecnológicas (*Apple, Google, Amazon, Facebook* y *Microsoft*) son estadounidenses. Todas ellas se enfocan en el *big data* y controlan en su conjunto una gran parte de los datos generados a nivel mundial. Las empresas europeas tienden a confiar el almacenamiento, gestión y procesamiento de sus datos a dichas empresas.

De todo ello nace una fuerte dependencia de las empresas europeas respecto de Estados Unidos, situación que no es vista con buenos ojos en el seno de la Unión Europea, especialmente por el dúo que conforman Alemania y Francia.

Ante la gravedad de los hechos, parece que la UE comienza a reaccionar. Desde el 2018, la Comisión Europea ha ido fraguando una ambiciosa agenda digital con la finalidad de poner remedio a esta situación y recuperar la "soberanía digital" de la UE.

[21] El País. "Europa ultima un plan para dar la batalla en el negocio de los datos". (*El País*, 17-11-2019). Disponible en <https://elpais.com/economia/2019/11/16/actualidad/1573926886_318836.html> [Consulta: 11-02-2020].

Finalmente, el pasado 19 de febrero de 2020, la Comisión reveló su estrategia para la consecución de tales objetivos en los próximos años, con la presentación del Libro Blanco de la Inteligencia Artificial y la Estrategia Europea de Datos.[24]

A la cabeza de todo este proyecto se encuentra Margrethe Vestager, comisaria de Competencia y vicepresidenta ejecutiva para una Europa Adaptada a la era digital, a la que se había encomendado el diseño e implementación de una estrategia de inteligencia artificial y *big data*.[25]

Los altos mandatarios de la UE consideran que Europa dispone de todos los ingredientes necesarios para liderar a nivel mundial en los sistemas de inteligencia artificial y en la nueva economía de los datos.

El objetivo en este último ámbito es la creación de un "Espacio Europeo de Datos"; es decir, la unificación del mercado de los datos en el marco de la UE.[26] La idea es fomentar la libre circulación de los datos no personales entre Administraciones Públicas, investigadores, empresas y ciudadanos. Con ello se pretende dar solución a una de las mayores limitaciones que ralentiza actualmente el desarrollo digital en la UE: la disponibilidad de datos para la innovación y desarrollo de la inteligencia artificial.[27]

Una muestra de este nuevo impulso europeo es Gaia-X, el proyecto para conseguir una nube europea lanzado conjuntamente por Alemania y Francia, desvelado el 30 de octubre del pasado 2019.[28] El fundamento del proyecto es tratar de reducir la dependencia europea garantizando a las empresas y Administraciones Públicas europeas la posibilidad de almacenar y gestionar sus datos en Europa.[29]

El panorama descrito requiere de una actualización del Derecho existente, que se adapte a las necesidades de un entorno cambiante donde los datos y la inteligencia artificial son dos

---

[24] Comisión Europea. *A European Strategy for Data.* COM(2020) 66 final (19-02-2020), p. 1.

[25] Comisión Europea (Comunicado de prensa). "Dar forma al futuro digital de Europa: la Comisión presenta sus estrategias en relación con los datos y la inteligencia artificial". (*Comisión Europea*, 19-02-2020). Disponible en <https://ec.europa.eu/commission/presscorner/detail/es/ip_20_273> [Consulta: 10-04-2020].

[26] Comisión Europea, *A European Strategy*…, cit., p. 4.

[27] Ibid, p. 6.

[28] El Confidencial. "Alemania inaugura el pulso con EEUU para lograr la "soberanía digital" de la UE". (*El Confidencial,* 17-11-2019). Disponible en <https://www.elconfidencial.com/economia/2019-11-17/alemania-inaugura-el-pulso-con-eeuu-para-lograr-la-soberania-digital-de-la-ue_2339299/> [Consulta: 11-2-2020].

[29] Ibid.

ingredientes básicos. Esta reforma debe abordarse desde las áreas jurídicas que ya hemos mencionado: derecho del consumo, derecho de la protección de datos y derecho de la competencia.

La intervención de este último elemento es aún bastante controvertida. Hasta hace poco, no se consideraba que el *big data* pudiese acarrear conflictos desde la perspectiva competitiva. No obstante, parece que la Comisión Europea está cambiando de opinión. Prueba de ello es el proceso iniciado contra a *Google* por abuso de posición dominante, que ha concluido con una sanción millonaria.[30]

Habrá que analizar, en un futuro, la adecuación de los instrumentos jurídicos europeos (artículos 101, 102 y 107 del TFUE y Reglamento (CE) 139/2004 o "Reglamento Europeo de Concentraciones") para combatir las conductas anticompetitivas derivadas del uso de *big data*. La reforma legislativa en esta área jurídica llevada a cabo en Alemania en 2017 puede utilizarse como modelo.[32]

El Derecho del consumo en la UE se conforma por un entramado de normas dominado por la Directiva 2011/83/UE, sobre los derechos de los consumidores.[33] La reciente Directiva modificativa (UE) 2019/2161 amplía su ámbito de aplicación para abarcar servicios o contenidos digitales en los que el consumidor proporciona datos personales. Recientemente, la Directiva (UE) 2015/2366, sobre servicios de pago en el mercado interior[34] y la Directiva (UE) 2019/770 relativa a determinados aspectos de los contratos de suministro de contenidos y servicios digitales[35] atribuyen nuevos derechos a los consumidores relativos al tratamiento de datos de carácter personal en el marco de la economía digital.

En cualquier caso, la protección del consumidor en materia de *big data* es un área de choque con la normativa de protección de datos. En consecuencia, la protección al consumidor en este ámbito queda fundamentalmente canalizada a través del RGPD.

---

30 Decisión de la CE, de 20 de marzo de 2019, caso AT.40411 *Google Search (AdSense)*.

32 BUDZINSKI, op. cit., p. 15.

33 Directiva 2011/83/UE del Parlamento Europeo y de Consejo de 25 de octubre de 2011 sobre los derechos de los consumidores.

34 Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015 sobre servicios de pago en el mercado interior.

35 Directiva (UE) 2019/770 del Parlamento Europeo y del Consejo, de 20 de mayo de 2019, relativa a determinados aspectos de los contratos de suministro de contenidos y servicios digitales.

En lo que respecta al Derecho de protección de datos, la UE se ha convertido en un referente mundial a raíz de la entrada en vigor del citado RGPD, el 25 de mayo de 2018.

Sin duda, el RGPD juega un papel central en el entramado de la Estrategia Europea de Datos, tratándose del primer instrumento europeo especializado en la protección de datos desde la óptica del *big data*. La Comisión ha afirmado que, con este instrumento, ha creado un "sólido marco para la confianza digital",[36] aplicable a todos los ciudadanos de la Unión y con trascendencia más allá de sus fronteras.

Por consiguiente, es en este instrumento jurídico donde se debe poner el énfasis. Por ello, analizaremos sus novedades y particularidades, los puntos de debate más candentes y su pretendido carácter internacional, para finalizar estableciendo algunas recomendaciones.

5. MARCO JURÍDICO DE LA PROTECCIÓN DE DATOS

5.1. Los orígenes de la protección de datos en la Unión Europea.

El derecho a la protección de datos surge como una subcategoría del derecho a la privacidad,[37] cuyo objetivo fundamental es garantizar el poder de disposición y control del ciudadano sobre sus datos personales.[38]

Consciente de su relevancia, la UE otorga reconocimiento jurídico a este derecho al más alto nivel. Así, el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea y el artículo 16 del Tratado de Funcionamiento de la Unión Europea (TFUE) recogen expresamente que "toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan".[39]

La primera norma europea en esta materia fue la Directiva 95/46/CE de Protección de Datos de 24 de octubre de 1995. Esta norma estaba fuertemente influenciada por el Convenio 108 para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal, adoptado por el Consejo de Europa en 1981, y respondía

---

[36] Comisión Europea, *A European Strategy*…, cit., p. 4.

[37] ALIBEIGI, Ali; MUNIR, Abu Bakar; ERSHADULKARIM, MD y ASEMI, Adeleh. "Towards standard information privacy, innovations of the new General Data Protection Regulation". *Library Philosophy and Practice* (revista electrónica), núm. 2840, 2019, p. 2.

[38] Acorde con la definición en la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre de 2000.

[39] Artículo 8 de la Carta de Derechos Fundamentales de la UE y artículo 16 del Tratado de Funcionamiento de la Unión Europea.

obviamente al estado de la cuestión en la época, con un desarrollo muy incipiente de Internet y del tratamiento digital de datos.

En España, la trasposición de esta Directiva se realizó a través de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su Reglamento de desarrollo, el Real Decreto 1720/2007, de 21 de diciembre.[40]

Aparte de estas normas jurídicas de carácter vinculante, hemos de destacar los documentos e informes publicados por el Grupo de Trabajo creado en virtud del artículo 29 de la Directiva ("GT29"). En base a dicho artículo, el Grupo tendría "carácter consultivo e independiente"[41] y estaría conformado -entre otros- por un representante de la autoridad de control competente de cada Estado Miembro.

A este Grupo se deben una serie de documentos e informes que encuentran su reflejo en el RGPD.

5.2. El Reglamento General de Protección de Datos.

La Directiva había quedado obsoleta. En su sustitución nace el RGPD nace debido a las necesidades acuciantes de un nuevo entorno caracterizado por la digitalización de la economía y la vida social. En este entorno, la escala a la que se realizan intercambios de datos personales ha crecido exponencialmente. Ello plantea nuevos desafíos a resolver por las normas de protección de datos, que tratan de conjugar el derecho a la privacidad de los individuos con la libre circulación de los datos.

El RGPD trata de reforzar el control de los usuarios de sus propios datos personales. Hablamos del *empoderamiento* del individuo, a través de un sistema donde consentimiento informado juega un papel central.

Sin embargo, el derecho a la privacidad de datos no es un derecho absoluto, sino que debe considerarse en relación a otros principios y derechos, con arreglo al principio de proporcionalidad.[42]

Las empresas, a pesar de ser objeto de mayores cargas, también se verían beneficiadas gracias al Reglamento. La mayor confianza de los consumidores, la claridad y unificación de

---

[40] Derogada por la actual Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

[41] Artículo 29.1. de la Directiva.

[42] 4º considerando del RGPD.

criterios en la Unión Europea y la introducción de mecanismos simplificadores como el de "ventanilla única" son algunas de las ventajas que ofrece.

Acorde a sus pretensiones de situarse a la cabeza de la revolución tecnológica, la UE requería un nuevo marco jurídico. Este marco ha de facilitar la libre circulación de los datos tanto dentro del territorio de la UE como entre la UE y terceros países. Para ello, era necesario fijar estándares de privacidad claros y homogéneos en todo el territorio de la Unión. La unificación de estándares también supondría un gran ahorro en costes monetarios. La Comisión ha estimado un ahorro de unos 2,3 billones de euros al año bajo la nueva legislación.[43]

El Preámbulo del RGPD explica estos objetivos y justifica además la elección del reglamento -en lugar de la directiva- como instrumento jurídico óptimo para llevar a cabo esta tarea.

El reglamento es una norma jurídica vinculante, directamente aplicable en todo el territorio de la UE desde el momento en que entra en vigor. Por el contrario, la directiva obliga a todos los países de la UE a cumplir un determinado objetivo, correspondiendo a cada uno de los Estados tomar decisiones sobre cómo alcanzarlos. Es decir, una directiva obliga en los fines, pero deja libertad en cuanto a los medios.

La derogada Directiva ha dado lugar a distintos niveles de protección de datos en cada uno de los países miembros de la UE, dificultando la libre circulación de datos personales entre ellos. Con el Reglamento se pretende crear un marco jurídico más "sólido y coherente"[44] en todo el territorio de la UE, lo que implica evitar las diferencias en la trasposición causadas por la antigua Directiva. No obstante, el RGPD sigue reconociendo un "margen de maniobra"[45] a los Estados Miembros a la hora de la incorporación y adaptación a su propio Derecho. Por ejemplo, el Reglamento deja a la libertad de los Estados la configuración de un umbral de protección más exigente en relación a la categoría de los "datos sensibles", como puede apreciarse en la LOPD.[46]

---

[43] Comisión Europea. "Questions and Answers-General Data Protection Regulation". (*Comisión Europea*, 2019). Disponible en <https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_387> [Consulta: 16-02-2020].

[44] 7º considerando del RGPD.

[45] 10º considerando del RGPD.

[46] El artículo 7.2 de la LOPD obliga al consentimiento expreso y por escrito del interesado, mientras el artículo 9.2.a) del RGPD solo exige el consentimiento explícito del interesado.

6. NOVEDADES DEL RGPD

La revolución del *big data* y sus posibilidades han dado lugar a un encarnizado debate: ¿A quién pertenecen los datos?

La cuestión del derecho de propiedad sobre los datos de carácter personal no es fácil de dilucidar;[47] aunque parece que el Reglamento se decantaría por el derecho de propiedad del individuo sobre sus datos frente a las empresas responsables de su tratamiento. Esta lógica sería coherente con el afán de dicha Norma por reforzar el control que los usuarios tienen sobre los mismos.[48]

La reforma se fundamenta en dos pilares: el consentimiento informado y el principio de transparencia. Asimismo, el Reglamento refuerza el papel del individuo en la protección de sus datos de carácter personal mediante la creación de nuevos derechos, como son el derecho a la portabilidad de los datos y el derecho al olvido.

En lo que se refiere a las empresas, estas son objeto de nuevas obligaciones que encuentran su fundamento en el principio de responsabilidad proactiva. Para complementarlo, las infracciones de la nueva normativa serán sancionadas mucho más severamente.

A continuación, nos esforzaremos por identificar los puntos clave de la reforma, analizando su significado y esbozando algunas de las controversias que sobre ellos se ha generado o pueden llegar a generarse.

Para facilitar el análisis, vamos a diferenciar cinco bloques de provisiones en función de su contenido. Nos referiremos primero a las novedades en el ámbito material y territorial de la nueva legislación. Continuaremos con aquellas medidas que tienen por objeto incrementar el control del individuo sobre sus datos; a este segundo bloque dedicaremos una especial atención. Seguiremos repasando las nuevas obligaciones y cargas a las que se enfrentan las empresas, para finalizar haciendo una pequeña referencia a otras novedades y mecanismos.

6.1. Ámbito material.

[47] GIL, Elena. "*Big data*, privacidad y protección de datos". *Agencia Española de Protección de Datos*, 2015. Disponible en <https://www.aepd.es/sites/default/files/2019-10/big-data.pdf>, p. 139.

[48] La intención de reforzar el papel del individuo en el control de sus datos se aprecia ya en la exposición de motivos del RGPD, concretamente en el 11º considerando del RGPD.

Para entender el ámbito material de aplicación del RGPD, hemos de distinguir los conceptos de datos de carácter personal, datos pseudónimos y datos anónimos. En esta distinción es especialmente relevante la doctrina elaborada por el GT29.[49]

El RGPD es de aplicación a los procesos de tratamiento de datos de carácter personal, tal como quedan definidos en el artículo 4.1. Se entiende que son datos de carácter personal "toda información sobre una persona física identificada o identificable",[50] considerando que una persona física es identificable cuando su 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".[51]

La definición no ha experimentado grandes cambios en respecto a la precedente Directiva, salvando la enumeración de nuevos "identificadores", como los datos de localización o la identidad genética del individuo.

A *sensu contrario*, el Reglamento excluye a aquellos datos que hayan sido anonimizados; es decir, que pertenecen a individuos no identificables. El GT29 ha concluido que cuando una base de datos ha sido completamente anonimizada el Reglamento no es de aplicación.[52]

Las ventajas de la anonimización para los responsables del tratamiento de datos son evidentes, pues se ahorrarían todos los inconvenientes derivados de la necesidad de recabar el consentimiento del individuo, las restricciones en la posibilidad de transmitir estos datos a terceros, el cumplimiento de las obligaciones que impone la normativa, etc.

La anonimización de datos es por definición un proceso irreversible a través del cual se hace imposible la reidentificación del sujeto. El problema es que el *big data* incrementa el riesgo de reidentificación de los usuarios, incluso una vez se han aplicado técnicas de anonimización sobre los datos.

Por ello, hay que distinguir entre dos formas de entender la anonimidad de los datos: anonimización absoluta o anonimización funcional. Mientras que la primera entiende que los

---

[49] GT29. *Opinion 05/2014 on Anonymisation techniques.* 0829/14/EN WP216 (10-04-2014).

[50] Artículo 4.1 del RGPD.

[51] Artículo 4.1 del RGPD.

[52] GT29, *Opinion 05/2014 …,* cit.

datos son anónimos cuando no existe posibilidad alguna de reidentificar a los sujetos, la segunda entiende que existe un riesgo mínimo de reidentificación.

Teniendo en cuenta la imposibilidad práctica de aplicar el primer criterio, el GT29 parece adoptar por norma la anonimización funcional.[53] Esto es, se entiende que los responsables del tratamiento han anonimizado los datos cuando el riesgo de reidentificación, sin ser cero, es prácticamente inexistente.

No obstante, este proceso es que podría restar tanto valor a los datos como para hacerlos inservibles para el responsable del tratamiento. Aquí entra en juego el concepto de la pseudonimización. Los datos pseudónimos son definidos como aquellos datos que no pueden atribuirse a una persona sin utilizar información adicional.[54] Las técnicas más frecuentes de pseudonimización de datos son la encriptación, la función *hash* y la *tokenización*.[55]

A diferencia de la anonimización, la pseudonimización es un proceso reversible; existe la posibilidad de reidentificar a los sujetos, siempre que se disponga de la información adicional que permite relacionar al individuo con el dato seudónimo.

Luego en aquellos casos en que no se alcance el umbral de la anonimicidad, nos encontraríamos ante datos pseudónimos. Para analizar si nos encontramos ante datos pseudónimos o ante datos anónimos, el GT29 ha elaborado dos métodos alternativos:

1. Realizar un estudio del riesgo de reidentificación.
2. Una base de datos será anónima cuando no exista posibilidad de singularizar a un individuo (*singling out*), capacidad de inferir nuevos datos sobre los usuarios (*inference*) o capacidad de asociar datos a un mismo individuo (*linkability*).[56]

El GT29 concluyó en su estudio que muchas empresas, pretendiendo crear una base de datos anónimos, obtienen en su lugar datos pseudónimos. Es decir, los datos pertenecen a personas que pueden ser identificables a través de alguna de las técnicas a que acabamos de hacer referencia. En consecuencia, estos datos sí estarían sometidos a la regulación del Reglamento.

---

[53] GIL, Elena, op. cit., p. 86.

[54] Artículo 4.5 del RGPD.

[55] PLATH, Sylvia. "And I sit here without identity: faceless. My head aches" (*PwC Luxembourg*, 2016). Disponible en <https://www.pwc.lu/en/general-data-protection/docs/pwc-anonymisation-and-pseudonymisation.pdf> [Consulta: 17-2-2020].

[56] GIL, Elena, op. cit., p. 102.

La pseudonimización figura en el RGPD como una de las técnicas de las que pueden hacer uso responsables y encargados del tratamiento a la hora de garantizar la seguridad de los datos.[57]

Generalmente, los procedimientos de pseudonimización se llevan a cabo en el ámbito sanitario y farmacéutico, con la finalidad de proteger los datos relativos a la salud de los pacientes (los cuales entran en la categoría de "datos sensibles"). Un ejemplo de aplicación de esta técnica sería la sustitución del nombre de los pacientes de la base de datos de un hospital por un identificador numérico.

6.2. Ámbito territorial.

Uno de los rasgos más destacables del Reglamento es su marcado carácter extraterritorial. En otras palabras, el Reglamento no se aplica exclusivamente a las empresas cuyo domicilio social se encuentre en Europa.

Por virtud del artículo 3.2, el Reglamento será de aplicación al tratamiento de datos personales de residentes de la UE por parte de empresas que oferten bienes o servicios -con independencia de que medie o no un pago monetario- o controlen el comportamiento de los usuarios en el territorio de la UE.[58]

Dos buenos ejemplos de empresas a las que se aplicaría el Reglamento por virtud del artículo 3.2 son *Amazon* (que oferta bienes y servicios a residentes de la UE) y *Google Analytics* (que ofrece servicios de control o análisis del comportamiento de los usuarios de la UE en páginas web).[59]

Bajo la antigua regulación, las empresas europeas estaban sometidas a estándares de privacidad mucho más estrictos que aquellas empresas que, operando en el territorio de la UE, estaban establecidas en el exterior de la Unión. En este sentido, la Comisión Europea entiende que la extraterritorialidad de la nueva norma eliminará la ventaja de la que gozaban estas últimas (en particular, las grandes tecnológicas estadounidenses) y equilibrará el campo de juego entre todas las empresas; incrementando la competitividad de las empresas europeas.[60]

---

[57] Artículo 32 del RGPD.

[58] Artículo 3.2 del RGPD.

[59] Signaturit. "GDPR: ¿qué necesitas saber del nuevo Reglamento Europeo de Protección de Datos?" (*Signaturit*, 2018). Disponible en <https://blog.signaturit.com/es/las-claves-sobre-el-nuevo-reglamento-europeo-de-proteccion-de-datos> [Consulta: 18-2-2020].

[60] Comisión Europea, *Questions and Answers…,* cit.

6.3. El reforzamiento del papel del individuo.

6.3.1. El consentimiento informado.

El consentimiento informado es la columna vertebral de un modelo diseñado para proporcionar un mayor control a los individuos sobre sus datos de carácter personal. El RGPD refuerza la importancia del consentimiento del usuario en el escenario de la protección de datos a la par que incrementa los requisitos exigibles para que dicho consentimiento sea válido.

El consentimiento es una de las bases jurídicas -no la única, si bien la más debatida- que justifica el tratamiento de los datos de carácter personal del individuo. El artículo 4.11 del RGPD lo define como una "manifestación de voluntad libre, específica, informada e inequívoca" que implica una "declaración o clara acción afirmativa" por parte del usuario que acepta el tratamiento.

Para considerarse "libre", el consentimiento ha de manifestar una verdadera elección por parte del individuo. Por tanto, la ejecución de un contrato no puede depender del consentimiento del contratante al procesamiento de datos personales no necesitados para dicha ejecución (prohibición de conductas de *tying* o *coupling).*[62]

El consentimiento es informado y específico cuando el usuario conoce cierta información como la identidad del responsable del tratamiento, el tipo de información que será procesada, los fines a los que se destinará dicha información, los derechos de los que goza (como el derecho a retirar su consentimiento en cualquier momento) o los riesgos a los que se enfrenta.[63]

El consentimiento debe otorgarse para cada uno de los fines a los cuales se dirige el tratamiento. Si el tratamiento tiene varios fines, el usuario debe consentir para cada uno de ellos. En la práctica, surge un problema cuando las propias empresas no tienen conocimiento exacto de a qué fines serán destinados los datos, como suele suceder en el ámbito de la investigación científica. Aquí se encuentra la base de la controversia sobre la relación entre protección de datos e investigación científica, que exploraremos más adelante.

El RGPD introduce un nuevo requisito para que el consentimiento sea válido, y es que este ha de ser "inequívoco"; es decir, no ambiguo. Este requisito enlaza directamente con la

---

[62] GDPR-info. "GDPR-consent". (*GDPR-info*, s.f.). Disponible en <https://gdpr-info.eu/issues/consent/> [Consulta: 18-2-2020].

[63] Artículo 13 del RGPD.

expresa mención a la necesidad de "una declaración o clara acción afirmativa"[64] por parte del usuario.

Sin duda alguna, este es el cambio más significativo de la nueva legislación. Antes de la entrada en vigor de esta norma, existía un debate acerca de qué forma de manifestación del consentimiento era más adecuada: los sistemas de *opt-in* o los sistemas de *opt-out*.[65]

Los sistemas de *opt-in* exigen una acción o consentimiento expreso por parte del usuario cuyos datos personales pretenden tratarse. Por su parte, los sistemas *opt-out* se basan en la presunción del consentimiento, de manera que el usuario ha de manifestar expresamente su negativa al tratamiento de sus datos personales.

Precisamente, una de las mayores preocupaciones de los usuarios era que sus datos personales fuesen utilizados por las compañías que les ofrecían bienes y servicios sin su consentimiento. Para dar solución a este problema, el RGPD optó por incluir expresamente la necesidad de que el usuario manifieste su consentimiento mediante una acción o declaración afirmativa, esto es, mediante un sistema *opt-in*.

El RGPD reconoce que este consentimiento puede manifestarse rellenando una casilla en una página web.[66] En base a esta premisa, las empresas que operan *online* han resuelto la prestación del consentimiento a través de las denominadas "políticas de privacidad", que no dejan de ser fuente de numerosas controversias, como también veremos.

6.3.2. El principio de transparencia.

El artículo 5 del RGPD reconoce una serie de principios relativos al tratamiento de los datos personales ya enumerados en la Directiva. Estos son los principios de licitud y lealtad del tratamiento, limitación de la finalidad y del plazo de conservación, minimización de datos y exactitud.

A estos se suman otros destinados a incrementar la responsabilidad de la empresa, donde podemos anclar los principios de integridad y confidencialidad, así como el fundamental principio de responsabilidad proactiva.[67]

---

[64] 11º considerando del RGPD.

[65] GIL, Elena, op. cit., p. 79.

[66] 32º considerando del RGPD.

[67] Artículo 5.2 del RGPD.

Coherente con la intención de incrementar el control del individuo sobre sus datos, el RGPD incorpora a mayores el principio de transparencia.[68] Este principio, del que se empapa el resto de la regulación, implica que toda la información que se proporciona al sujeto ha de ser fácilmente accesible y entendible, en un "lenguaje sencillo y claro".[69]

Aplicado al tratamiento de los datos, este principio significa, entre otras cosas, informar al usuario de los fines a los cuales van a destinarse los datos recabados.[70] Por otro lado, el principio de transparencia lleva a fomentar el desarrollo de mecanismos de certificación y sellos de protección de datos.[71]

Con ello, se pretende evitar otro de los grandes temores de los usuarios, como son los usos oscuros que las empresas responsables y encargadas del tratamiento pueden hacer con sus datos personales.

6.3.3. El "derecho al olvido".

Aparte de otros que ya existían con anterioridad (como el derecho de acceso, el derecho a la información o el derecho a la rectificación de los datos), el RGPD reconoce dos nuevos derechos que han causado gran impacto en el ámbito de la protección de datos. Hablamos del "derecho al olvido" y el derecho a la portabilidad de los datos. Mientras el primero afectaría de manera más significativa a los buscadores de Internet, como *Google*; el segundo afectaría en el ámbito de las redes sociales, como *Facebook*.

El derecho al olvido fue reconocido por el Tribunal de Justicia de la Unión Europea (TJUE) en la sentencia del caso *Google Spain*,[72] en 2014.

El origen del asunto se encuentra en la negativa de *Google* a eliminar de su buscador ciertos datos que el reclamante, Mario Costa González, consideraba obsoletos y sin interés público; pero que le causaban perjuicio. En concreto, Costa exigía la retirada de un artículo

[68] Artículo 12 del RGPD.

[69] 39º considerando del RGPD.

[70] Artículos 13 y 14 del RGPD.

[71] Artículos 40-43 del RGPD.

[72] Sentencia del Tribunal de Justicia de la UE de 13 de Mayo de 2014, caso C-131/12 *Google Spain SL v. Agencia Española de Protección de Datos*.

periodístico de 1998 en el que se hacía mención al embargo de un inmueble de su propiedad. Tras interponer distintas acciones legales en España,[73] el asunto llegó a las manos del TJUE.

El TJUE decidió resolver en favor de Mario Costa. Dicha decisión contiene un reconocimiento clave de los derechos que un individuo ostenta frente a los responsables del tratamiento de datos. A solicitud del usuario, la empresa responsable del tratamiento tiene la obligación de suprimir sus datos de carácter personal cuando estos ya no sean necesarios para la finalidad para la que se recogieron, cuando el usuario retire su consentimiento o se oponga al tratamiento, o cuando los datos inicialmente hubieran sido tratados ilícitamente.[74] Este es el contenido del tradicional derecho a la supresión de los datos, que ya reconocía la Directiva.

"El derecho al olvido" es la manifestación del derecho a la supresión de los datos cuando el responsable del tratamiento es un buscador de Internet que ha hecho públicos los datos. En este caso, el responsable ha de asegurarse de eliminar de su lista de resultados los enlaces a sitios web que contengan la información que el individuo desea suprimir[75] y adoptará "medidas razonables" para informar acerca de la solicitud de supresión a dichos sitios web.[76]

El reconocimiento de este derecho impone una pesada carga sobre los motores de búsqueda. En respuesta inmediata a la decisión del TJUE, *Google* introdujo un formulario a disposición de los usuarios para solicitar la eliminación de información personal amparada por el derecho al olvido. Ya en 2014, *Google* recibió más de medio millón de solicitudes.[77]

6.3.4. El derecho a la portabilidad de los datos.

El artículo 20 del RGPD desarrolla el concepto de la portabilidad de los datos, que consiste simplemente en la transmisión de datos de carácter personal de un responsable del tratamiento de los datos a otro, a solicitud del individuo. El interesado tiene derecho a recibir

---

[73] Costa interpuso una acción ante la Agencia Española de Protección de Datos (AEPD), que reconoció efectivamente su "derecho al olvido". *Google* recurrió la decisión ante la Audiencia Nacional, y esta planteó una serie de cuestiones acerca de la interpretación de la entonces vigente Directiva al TJUE.

[74] Artículo 17.1 del RGPD.

[75] LOZANO GARROTE, Juan. "Derecho al olvido. La protección de datos frente a los motores de búsqueda como Google". (*Noticias Jurídicas*, 26-04-2019). Disponible en <http://noticias.juridicas.com/conocimiento/articulos-doctrinales/13910-derecho-al-olvido-la-proteccion-de-datos-frente-a-los-motores-de-busqueda-como-google/> [Consulta: 16-02-2020].

[76] Artículo 17.2 del RGPD.

[77] ÁLVAREZ RIGAUDIA, Cecilia. "Sentencia Google Spain y derecho al olvido". *Actualidad Jurídica Uría Menéndez*, núm. 38, 2014, p. 117.

los datos en un "formato estructurado, de uso común y lectura mecánica",[78] así como a la transmisión directa de responsable a responsable, siempre que esto sea posible.

La justificación del derecho a la portabilidad de los datos puede analizarse desde dos perspectivas.

Desde la perspectiva de la Protección de datos, este derecho refuerza el control de los individuos sobre sus datos personales. El impacto de la portabilidad de los datos se aprecia especialmente en las redes sociales, como *Facebook*. Si el coste de cambiar de una red social a otra es demasiado alto, el miedo a perder valiosa información personal forzará a los individuos en muchas ocasiones a mantenerse en la misma red social. Este es el denominado efecto *lock-in.*[79]

El derecho a la portabilidad de los datos cobra también un especial significado desde la perspectiva del Derecho de la competencia. En un mercado de competencia perfecta, los consumidores deberían tener la posibilidad de transmitir sus datos de carácter personal a voluntad propia. La Comisión Europea ha reconocido que el derecho a la portabilidad de los datos fomentará un mercado más competitivo en el marco de la Unión,[80] al facilitar a las pequeñas empresas emergentes (*start-ups*) introducirse en mercados donde gigantes como *Facebook* se encuentran ya consolidados. Estas nuevas empresas podrían tratar de atraer nuevos usuarios ofreciendo políticas de privacidad más atractivas; de manera que, reconocido este derecho a la portabilidad de los datos, muchos usuarios de otras redes considerarían la posibilidad del cambio.

Desde esta óptica, conductas de *lock-in* por parte de ciertos operadores podrían constituir un abuso de posición dominante tal como queda recogido en el artículo 102 TFUE. Concretamente, la negativa por parte de empresas que se encuentran en una posición de dominio de mercado a facilitar la portabilidad de los datos podría constituir una conducta excluyente de la competencia prohibida bajo dicha provisión.[81]

Los diferentes enfoques desde los que puede justificarse el derecho a la portabilidad de los datos generan un debate acerca de su naturaleza y alcance. Nos encontramos ante un área

---

[78] Artículo 20.1 del RGPD.

[79] DIKER VANBERG, Aysem y ÜNVER, Mehmet Bilal. "The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo?". *European Journal of Law and Technology,* vol. 8, núm. 1, 2017, p. 4.

[80] Comisión Europea, *Questions and Answers…,* cit.

[81] DIKER VANBERG, op. cit., p. 6.

a caballo entre el Derecho de la competencia, el Derecho del consumo y la Protección de datos.[82]

Todas estas perspectivas podrían ser compatibles, teniendo en cuenta las distintas funciones que desempeña portabilidad de los datos. Las normas de protección de datos y el derecho de la competencia podrían enriquecerse mutuamente; si bien para llegar aquí habría que solucionar ciertos puntos de conflicto existentes entre ambas áreas jurídicas. Por ejemplo, según el RGPD, el derecho a la portabilidad de los datos se refiere exclusivamente a los datos de carácter personal; mientras que, desde la perspectiva del derecho de la competencia hablaríamos de un concepto más amplio, no restringido estrictamente a esta categoría de datos.

6.3.5. Decisiones automatizadas y elaboración de perfiles.

Uno de los grandes peligros que genera el *big data* en el ámbito de la privacidad y los derechos del consumidor es la toma de decisiones automatizadas.

Con "decisiones automatizadas" nos estamos refiriendo a decisiones sobre los individuos tomadas sin intervención humana, más allá de la intervención necesaria para la fijación de los parámetros en que se basan los algoritmos que analizan los datos relevantes para llegar a una conclusión.[83]

El problema se agrava en sectores especialmente sensibles, como el bancario, el asegurador o sanitario.[84] Las decisiones tomadas en este tipo de ámbitos tienes una gran trascendencia para el individuo, pudiendo abarcar desde la concesión de un préstamo hasta un diagnóstico médico. Por eso, la toma de decisiones sobre una persona sin supervisión humana alguna en estos sectores quizá no sea la solución más adecuada.

Aunque los legisladores europeos -ya conscientes de esta problemática- introdujeron una provisión explícita para proteger a los individuos frente a este tipo de decisiones en la Directiva,[85] el RGPD ha ido más allá en diversos sentidos.

---

[82] KERBER, Wolfgang. "Digital markets, data, and privacy: competition law, consumer law and data protection". *Journal of Intellectual Property Law & Practice,* vol. 11, núm. 11, 2016, pp. 856-866.

[83] GIL, Elena, op. cit., p. 41.

[84] GIL, Elena, op. cit., p. 42.

[85] Artículo 15 de la Directiva.

Centrándonos en este último, el artículo 22 reconoce el derecho a "no ser objeto de una decisión basada únicamente en el tratamiento automatizado",[86] cuando la decisión produzca "efectos jurídicos en él o le afecte significativamente".[87]

El RGPD hace referencia a la "elaboración de perfiles" como una de las formas de tratamiento automatizado de datos prohibida. Basándonos en la definición de la Agencia Europea de los Derechos Fundamentales, la elaboración de perfiles consiste en la categorización de los individuos en base a determinadas características personales (su edad, género, hábitos, conducta, etc).[88] La elaboración de perfiles entraña un alto riesgo de discriminación hacia aquellos individuos que no se ajustan al perfil que se les ha asignado. De hecho, una de las enmiendas propuestas al artículo 22 del RGPD incluía una mención expresa a la prohibición de elaboración de perfiles que generasen discriminación.[89] La enmienda no ha sido finalmente incorporada; aunque, ciertamente, una referencia explícita a la prohibición de discriminación no hubiera estado de más.

El artículo 22.2 recoge distintas excepciones a la prohibición descrita en el apartado 1. El RGPD incorpora entre ellas el consentimiento explícito; nueva muestra del papel protagonista que juega este en el panorama de la protección de datos europeo. Asimismo, la excepción del consentimiento recalca la idea de que el verdadero peligro en la toma de decisiones automatizadas está en que el individuo no sea consciente de ello.

Una de las novedades más notorias en este ámbito se recoge en el artículo 22.3, que prohíbe la toma de decisiones automatizadas basadas únicamente en "datos sensibles" del individuo. Son "datos sensibles" del individuo aquellos referentes, por ejemplo, a la salud, orientación sexual, ideología o religión.[90] En cuanto estos datos afectan a la esfera más íntima y personal del individuo, es razonable que reciban una especial protección bajo el Reglamento.

6.3.6. El rol de las empresas: el principio de responsabilidad proactiva.

El RGPD incrementa notablemente el nivel de responsabilidad soportado por las empresas responsables del tratamiento de datos. El objetivo es hacer de ellas agentes más

---

[86] Artículo 22 del RGPD.

[87] Ibid.

[88] Agencia Europea de los Derechos Fundamentales. *Towards more effective policing -Understanding and preventing discriminatory ethnic profiling: a guide.* Oficina de Publicaciones de la Unión Europea, 2010, p. 8.

[89] GIL, Elena, op. cit., p. 129.

[90] Artículo 9.1 del RGPD.

conscientes de la delicadeza de los datos y de los riesgos que para la privacidad de los individuos entraña su tratamiento.

El Reglamento empuja a las empresas a colocar la privacidad y la seguridad de los datos personales en su punto de mira, tanto en el beneficio de los usuarios como en el suyo propio.

Estas cuestiones han de ser una prioridad a tener en cuenta en todas y cada una de las fases del proceso comercial, comenzando en el diseño de las tecnologías y continuando hasta el momento en que se termine la relación entre usuario y responsable del tratamiento, por el motivo que sea.

Eso sí, el RGPD concede un alto nivel de libertad a los responsables del tratamiento en la elección de los medios apropiados para garantizar el respeto a la privacidad y seguridad de los datos del individuo. Corresponde a las empresas evaluar cuál es el riesgo al que se enfrentan y adoptar las medidas técnicas y organizativas necesarias en consecuencia.

En línea con el mayor nivel de libertad concedida a las empresas y con el fin de agilizar el funcionamiento del sistema, se libera a las empresas de la obligación de notificar sobre sus actividades a las autoridades de control.[91] A cambio, los responsables han de llevar un registro de todas las actividades de tratamiento que lleven a cabo.[92]

Un mayor nivel de libertad suele implicar un mayor nivel de responsabilidad; y el Reglamento no es una excepción a la regla. Las empresas responsables del tratamiento han de ser consecuentes con sus actos y asumir los castigos que supone el incumplimiento de las normas.

Una de las críticas más compartida en relación a la antigua Directiva era la suavidad e insuficiencia de sus sanciones. El RGPD se ha endurecido significativamente en este aspecto, con la imposición de multas administrativas que pueden alcanzar los 20 millones de euros o hasta el 4% del volumen de negocio anual global de la empresa sancionada.[93]

6.3.7. El principio de responsabilidad proactiva (o *accountability*).

La inclusión del principio de responsabilidad proactiva entre los principios del tratamiento de los datos descritos en el artículo 5 es una señal muy evidente del papel tan activo que el RGPD reserva a las empresas responsables del tratamiento de los datos.

---

[91] 89º considerando del RGPD.

[92] Artículo 29 del RGPD.

[93] Artículo 83.5 del RGPD.

La responsabilidad proactiva consiste nada más y nada menos que en el cumplimiento del resto de principios descritos en el mismo artículo 5. Además, la responsabilidad implica la carga de probar el cumplimiento de los mismos. La manera más fácil de superar la prueba de cumplimiento es demostrar la adhesión a un código de conducta[94] o mecanismo de certificación.[95]

El cumplimiento de todos y cada uno de los principios implica la toma de medidas organizativas y técnicas necesarias para garantizar la seguridad en el tratamiento de los datos. El RGPD deja a discreción de las empresas la elección de los métodos más adecuados para asegurar el tratamiento de los datos, promoviendo técnicas como la anonimización, pseudonimización o encriptación de los datos.

Más allá de estos principios, el principio de responsabilidad proactiva se concreta en una serie de obligaciones impuestas sobre las empresas.

Aquí, hemos de distinguir entre dos tipos de obligaciones distintas:[96]

- Obligaciones fundamentadas en la privacidad de los individuos.
- Obligaciones fundamentadas en el riesgo.

A continuación, examinaremos cada uno de estos grupos.

6.3.8. Obligaciones fundamentadas en la privacidad.

Este conjunto de obligaciones encuentra su origen en el reconocimiento de los derechos de privacidad del individuo a los que ya nos hemos referido. Cada uno de ellos (derecho a la supresión y al olvido, acceso y portabilidad de los datos, derecho de oposición y rectificación) exige de las empresas responsables del tratamiento un esfuerzo por garantizarlos. Estamos ante la "otra cara de la moneda" de la privacidad.

El principio de transparencia se traduce para las empresas en un deber de información transparente. Básicamente, las empresas deben mantener informado en todo momento al usuario acerca del tratamiento de sus datos; y deben hacerlo utilizando un lenguaje claro y sencillo. Los requisitos informativos previos a la prestación de consentimiento son más exigentes ahora, y la carga de la prueba de consentimiento por parte del usuario recae en la empresa responsable del tratamiento.

---

94 Artículo 40 del RGPD.

95 Artículo 42 del RGPD.

96 Comisión Europea, *Questions and Answers…,* cit.

Mediante estas exigencias, el Reglamento trata de zanjar los debates acerca de la eficacia de las "políticas de privacidad", el medio más utilizado por las empresas que operan *online* para la prestación de consentimiento. El objetivo es que dichas políticas proporcionen un mayor nivel de información al usuario, y que esta información sea fácilmente accesible y entendible por cualquiera.

6.3.9. Obligaciones fundamentadas en el riesgo.

La violación de la seguridad de los datos puede entrañar daños tanto materiales como inmateriales para los individuos, incluyendo, entre otros, daños físicos, discriminación, usurpación de identidad o pérdidas económicas.[97] Ante tales riesgos, parece razonable que las empresas tomen precauciones suficientes en lo que se refiere al tratamiento de datos.

Sin duda, las nociones de privacidad por defecto y privacidad desde el diseño ocupan un rol predominante en este panorama. Obligaciones complementarias son la evaluación del impacto de riesgo y la notificación y comunicación ante una violación de la seguridad.

- Privacidad por defecto y privacidad desde el diseño.

En una cultura empresarial informada por estos principios las empresas tendrían menos dificultades en el cumplimiento de sus obligaciones. Este es el fundamento que subyace en el artículo 25 del RGPD.

El término de privacidad por defecto implica la preprogramación de una tecnología de la forma más protectora para la privacidad del usuario. La selección de un nivel de protección de datos menor estaría en manos del individuo, haciéndole responsable con ello de su decisión. La intención, según el artículo 25.2, es que "solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento".[98]

Por su parte, el término de privacidad desde el diseño hace referencia a la consideración de la protección de datos en el diseño y construcción de las tecnologías. La idea es que los diseñadores de tecnologías incluyan la protección de datos como uno de los factores determinantes en la construcción del modelo (junto a otros factores tradicionalmente considerados por los empresarios, como puede ser la viabilidad económica del negocio).

---

[97] 86º considerando del RGPD.

[98] Artículo 25.2 del RGPD.

Una combinación de ambos modelos llevaría a seleccionar por defecto las opciones más protectoras de la privacidad del individuo en una tecnología diseñada desde la lógica de la protección de datos personales.[99]

Por lo que respecta a su implementación, el artículo 25 se refiere a la necesaria toma de "medidas técnicas y organizativas" por parte de los responsables del tratamiento de los datos. Aunque con buenas intenciones, el RGPD no resuelve las dudas acerca de qué métodos se han de utilizar para esta tarea. La incertidumbre es mayor en relación a la privacidad desde el diseño, donde el único ejemplo de medida apropiada citado por la legislación es la pseudonimización de datos.

En cualquier caso, la referencia a dos tipos diferentes de medidas, técnicas y organizativas, indica que han de aplicarse tanto en el diseño de elementos del *hardware* o *software* como en los modelos de negocio y prácticas organizativas de la empresa. Por ejemplo, las reglas organizativas que determinan en qué supuestos y bajo qué condiciones puede un empleado acceder a determinadas categorías de datos.[100]

- Evaluación de impacto del riesgo.

En caso de que el tratamiento de datos "entrañe un alto riesgo para los derechos y libertades de las personas físicas",[101] el responsable del tratamiento tendrá la obligación de realizar una "evaluación del impacto de las operaciones de tratamiento en la protección de datos personales".[102]

- Notificación y comunicación ante la violación de seguridad.

La violación de la seguridad de los datos personales puede entrañar graves consecuencias para los individuos. Por ello, una vez se ha producido efectivamente la violación, es importante que los responsables del tratamiento de datos reaccionen con rapidez.

Acorde con el principio de transparencia, el Reglamento impone nuevas obligaciones tras la violación de datos a las empresas.

El artículo 33 exige al responsable del tratamiento la notificación a la autoridad competente de cualquier violación que pueda suponer un "riesgo" para los derechos y

---

[99] GIL, Elena, op. cit., p. 136.

[100] BOARDMAN, Ruth; MULLOCK, James y MOLE, Ariane. "Guide to the General Data Protection Regulation". *Bird & Bird*, 2017, p. 104.

[101] Artículo 35 del RGPD.

[102] Ibid.

libertades del individuo en un plazo de 72 horas. Asimismo, el artículo 34 exige la comunicación a los individuos afectados en caso de que la violación pueda entrañar un "alto riesgo" para sus derechos y libertades.

La cuestión es, ¿qué ha de entenderse por "riesgo o "alto riesgo" para los derechos y libertades del usuario? Ciertas categorías de datos, como aquellos que afecten a la salud del individuo o la información sobre una tarjeta de crédito o una cuenta bancaria entrañan sin duda un grave riesgo para los derechos de los individuos. Sin embargo, la diferenciación no siempre es tan evidente.

La ambigüedad afecta especialmente a algunos tipos de empresas, como aquellas dedicadas a la gestión de "la Nube".[103] Estas empresas podrían argumentar que su única función es almacenar información, sin entrar a valorar su contenido. La diferenciación entre información cuya difusión podría causar un "alto riesgo" para los derechos y libertades de los individuos se dificulta aún más en estos casos.

6.3.10. Delegado de protección de datos.

Los artículos 37-39 modelan esta nueva figura que ha de ser designada cuando la actividad principal de la empresa sea el tratamiento de datos (en atención a los requisitos del artículo 37). Es decir, el rasgo que hace necesaria la designación del delegado de protección de datos no es el tamaño de la empresa, sino la actividad principal de la misma.

La función del delegado es básicamente asesorar al responsable del tratamiento en materia de protección de datos y supervisar el cumplimiento de las obligaciones que le corresponden en este ámbito.

6.4. Otras novedades.

6.4.1. El Comité Europeo de Protección de Datos.

Este nuevo órgano se compone por el director de una autoridad de protección de datos de cada Estado miembro, además del Supervisor Europeo de Protección de Datos y el presidente.[104]

El Comité viene a sustituir al GT29, respecto al cual se distingue en cuanto a status. El GT29 no era más que un órgano consultivo cuya capacidad se limitaba a la elaboración de dictámenes e informes. A diferencia de su predecesor, el Comité es un organismo o

[103] ALIBEIGI, op. cit., p. 11.

[104] Artículo 68 del RGPD.

institución independiente de la UE, con personalidad jurídica propia y capacidad de adoptar decisiones vinculantes.[105]

Sus múltiples funciones pueden reconducirse a la elaboración de dictámenes, recomendaciones y directrices que guíen en la aplicación del Reglamento de forma coherente y homogénea en toda Europa.

En el cumplimiento de esta misión, el Comité tiene la facultad de dictar decisiones vinculantes en relación a las diferencias que puedan surgir a raíz del tratamiento transfronterizo de datos, para evitar las distintas soluciones al mismo problema que puedan darse en cada Estado Miembro.[106]

6.4.2. Mecanismo de "ventanilla única" (*one-stop-shop*).

El mecanismo de "ventanilla única" es de aplicación en caso de que el responsable o encargado del tratamiento de datos de carácter personal realice operaciones transfronterizas. El artículo 4.23 del RGPD entiende que una empresa opera más allá de sus fronteras bien cuando la empresa, teniendo establecimientos en más de un Estado Miembro, realiza operaciones de tratamiento de datos en varios de ellos; bien cuando la empresa, teniendo un único establecimiento en la UE, realiza operaciones de tratamiento que afectan sustancialmente a interesados en más de un Estado miembro.[107]

Cada una de dichas empresas se someterá al control de una "autoridad principal", que será aquella del Estado Miembro donde tenga su establecimiento principal o único establecimiento.[108]

Esto no excluye la posibilidad de que otras autoridades de control puedan tener cierta competencia sobre ellas. Para facilitar al ciudadano el ejercicio de sus derechos, se facilita la presentación de reclamaciones ante la autoridad de control de su país de residencia, siempre que la empresa concernida tenga un establecimiento o realice operaciones de tratamiento que afecten sustancialmente a individuos de ese país.[109]

---

105 Comité Europeo de Protección de Datos. "Acerca del CEPD". (*CEPD*, s.f.). Disponible en <https://edpb.europa.eu/about-edpb/about-edpb_es> [Consulta: 8-05-2020].

106 Comisión Europea. "¿Qué es el Comité Europeo de Protección de Datos (CEPD)?". (*Comisión Europea*, s.f.). Disponible en <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions/enforcement/what-european-data-protection-board-edpb_es> [Consulta: 23-2-2020].

107 Artículo 4.23 del RGPD.

108 Artículo 56.1 del RGPD.

109 Artículo 56.2 del RGPD.

En tales circunstancias, la autoridad de control informará a la autoridad de control principal; correspondiendo a esta última decidir si resolver el caso por sí misma o bien dejarlo en manos de la autoridad de control inicial.[110] En cualquier caso, corresponderá a esta última informar de la resolución al interesado.[111]

El razonamiento que subyace es la reducción de costes administrativos, la agilización y simplificación de los procesos y la aplicación más coherente del RGPD; sin imponer con ello ninguna carga adicional sobre los ciudadanos.

En la práctica, este mecanismo genera bastante confusión en cuanto a la identificación de la autoridad principal y la exigencia de un alto nivel de coordinación.

En respuesta al primer problema, el GT29 desarrolló en 2016 una serie de pautas diseñadas con la intención de facilitar la identificación de la autoridad principal.[112]

La mayor dificultad a día de hoy es cómo garantizar la cooperación, asistencia mutua y operaciones conjuntas entre las distintas autoridades de control nacionales a que hacen referencia los artículos 60 a 62 del Reglamento. El Reglamento no aporta ningún procedimiento o guía en concreto para facilitar este proceso, por lo que este es un reto que tendrán que afrontar las autoridades nacionales por sus propios medios.

Una vez superados estos obstáculos, las compañías podrían resultar altamente beneficiadas, ya que tendrían la posibilidad de desarrollar una estrategia de protección de datos personales más eficiente. Así, podrían diseñar una única estrategia aplicable por igual en todas sus oficinas, y el mecanismo se perfeccionaría con el tiempo debido al *feedback* aportado por la experiencia de cada una de ellas.[113]

7. PUNTOS MÁS CONTROVERTIDOS DEL RGPD

[110] Artículo 56.3 del RGPD.

[111] DE LA TORRE, Tanoj V. "Novedades, cambios y efectos del nuevo RGPD sobre la LOPD". *Inesem* (revista digital), 2017. Disponible en <https://revistadigital.inesem.es/juridico/nuevo-rgpd/>. [Consulta: 25-02-2020].

[112] GT29. *Guidelines for identifying a controller or processor's lead supervisory authority*. 16/EN WP244 (13-12-2016).

[113] Deloitte. "GDPR Top Ten #10: One Stop Shop". (*Deloitte*, s.f.). Disponible en <https://www2.deloitte.com/ch/en/pages/risk/articles/gdpr-one-stop-shop.html> [Consulta: 23-2-2020].

Hasta ahora, hemos expuesto las principales novedades que incorpora el RGPD. Nuestro objetivo a continuación es resaltar algunos de los puntos que han generado más controversia a propósito de su entrada en vigor.

Vamos a tratar de analizar la problemática en relación a tres cuestiones fundamentales:

- ¿Es el RGPD una limitación para la investigación científica?

- ¿Impone el RGPD una carga demasiado elevada para las empresas?

- ¿Es adecuado el sistema del consentimiento informado?

7.1. ¿Es una limitación para la investigación científica?

La tensión entre los distintos valores jurídicos que el Reglamento pretende equilibrar se hace especialmente palpable en el campo de la investigación científica. Con carácter previo a la entrada en vigor de esta norma, la preocupación sobre cómo influiría la nueva regulación en el campo de las ciencias y la innovación (especialmente, en el ámbito sanitario) se extendía entre los investigadores.

Particularmente, la cuestión surgía en torno a la dicotomía entre consentimiento y anonimización de los datos. Para entender la situación, vamos a centrarnos en un área concreta de la investigación biomédica especialmente conflictivo, cual es la genética.

La aplicación de las tecnologías de *big data* a la genética, a través de ciencias como la bioinformática y la genética computacional, ha revolucionado este campo en las últimas décadas.

Hasta hace pocos años, la investigación genética se limitaba a pequeñas muestras de un selecto número de pacientes, referidas a algún genoma individual. Ahora, algunos autores utilizan el término *big genetic data*,[114] para referirse a la utilización de bases de datos masivas que almacenan el genoma completo de miles de pacientes. Para ser de mayor utilidad aún, estas bases de datos suelen acompañarse de información relacionada con las características y hábitos de vida del paciente, como edad, sexo, raza, ocupación, etc.

El uso de estas grandes bases de datos trae consigo increíbles posibilidades para la ciencia, pero también implica grandes riesgos.

[114] QUINN, Paul y QUINN, Liam. "Big genetic data and its big data protection challenges." *Computer Law and Security Review,* vol. 34, núm.5, 2018, pp. 1000-1018.

Como ya vimos con anterioridad, la probabilidad de reidentificar a los individuos en bases de datos genéticas aparentemente anónimas se ha incrementado sustancialmente debido a ciertos avances tecnológicos (algoritmos cada vez más poderosos, interconectividad y acceso a bases de datos compartidas entre investigadores a nivel mundial, etc).[115] EL GT29 fija un umbral de anonimicidad especialmente elevado, de tal manera que no cabe posibilidad en la práctica de que las bases de datos genéticas puedan sean consideradas anónimas. En cualquier caso, tratar de alcanzar este umbral de anonimicidad llevaría en muchas ocasiones a la inutilidad de las bases de datos.

Este hecho plantea un problema para una práctica especialmente común en el campo de la investigación científica, cual es el uso secundario de las bases de datos genéticas. Hablamos de hacer accesibles y públicas para otros investigadores las bases de datos utilizadas en un proyecto, de tal manera que puedan ser utilizadas para otras investigaciones científicas posteriores. Esto supone un gran ahorro en tiempo y costes económicos, lo que facilita la innovación científica.

Si ya no cabe la posibilidad de garantizar la anonimicidad de las bases de datos genéticas, los datos que forman parte de las mismas entran en el concepto de "datos de carácter personal". Para ser más concretos, estos datos forman parte de una categoría especialmente protegida de datos, los llamados "datos sensibles", en los que se incluye toda la información relativa a la salud de un paciente.[116] En definitiva, dichas bases de datos se encuentran sometidas a las normas del RGPD.

Algunos de los principios que exige el RGPD no solo plantean dificultades de implementación, sino que además son directamente contradictorios con los propósitos de la investigación científica. Los principios de minimización de datos, limitación de la finalidad y limitación del plazo de conservación serían especialmente conflictivos. Ninguno de ellos parece compatible con algunas tendencias de la investigación genética como la creación de grandes bases de datos genéticas a largo plazo, cuyos datos pueden ser utilizados para distintas finalidades y "compartidos" entre distintas líneas de investigación.

Los derechos que la legislación proporciona a los sujetos también pueden llegar a imponer una carga muy onerosa sobre los investigadores. Garantizar el derecho de acceso no es tarea fácil. Como medida de seguridad, las bases de datos genéticas suelen estar agregadas o

[115] Ibid, p. 3.

[116] Artículo 9 del RGPD.

pseudonimizadas, lo cual dificulta considerablemente la reidentificación de los solicitantes que hacen uso de este derecho. Los derechos a la supresión y al olvido también chocan con los propósitos de la investigación, pues la eliminación de los datos de algunos individuos puede reducir la fiabilidad de los resultados e impedir la continuidad de proyectos que requieren todos los datos con los que se iniciaron.

El tratamiento de las bases de datos genéticas, como cualquier dato de carácter personal, exige la existencia de una base jurídica legítima. El artículo 9 prohíbe con carácter general el procesamiento de "datos sensibles", salvo que se cumpla una de las circunstancias que enumera el apartado 2. En lo que nos concierne ahora, nos interesan particularmente dos excepciones:

1. Consentimiento explícito, específico e informado del interesado.[117]
2. El tratamiento es necesario para fines de investigación científica (también llamada la "excepción de la investigación científica").[118]

El consentimiento del interesado constituía la piedra angular de la investigación científica bajo la antigua Directiva. Esta posición era respaldada por el GT29, por ser más aceptable desde el punto de vista ético y más acorde al principio de autonomía del paciente.[119]

Sin embargo, no parece que el consentimiento siga siendo el medio más adecuado sobre el que fundamentar la investigación científica legítima. La exigencia de un consentimiento explícito, informado y específico se hace casi imposible cuando ni siquiera los propios investigadores son conscientes de la finalidad que se dará a los datos o el tiempo que conservarán los datos en su poder. Muchos investigadores mostraban su preocupación y temían la ausencia de un "consentimiento genérico" (*broad consent*) que legitimase su actuación.

Consciente de las dificultades planteadas, el 33º considerando del Reglamento permite una especie de "consentimiento genérico", que consiste en el consentimiento del paciente "para determinados ámbitos de investigación científica que respeten las normas éticas reconocidas para la investigación científica".[120]

---

[117] Artículo 9.2.a) del RGPD.

[118] Artículo 9.2.j) del RGPD.

[119] GT29. *Working Document on the processing of personal data relating to health in electronic health records (EHR).* 00323/07/EN WP131 (15-02-2007).

[120] 33º considerando del RGPD.

La provisión es un pequeño alivio para los investigadores, pero en ningún caso pretende concederles un "cheque en blanco".[121] Primero, el 33º considerando no forma parte del articulado del Reglamento, con lo cual no es jurídicamente vinculante. Segundo, el potencial de esta provisión ha sido reducido por el GT29, al entender que cuando entren en juego los datos sensibles del artículo 9, el 33º considerando ha de ser objeto de interpretación estricta.[122] En definitiva, el consentimiento requerido para el artículo 9 ha de ser explícito, específico e informado; si bien estos requisitos se interpretarían con cierta flexibilidad en la luz de la investigación científica.

Todo parece indicar que la balanza se inclina hacia otras bases jurídicas para el tratamiento, como la excepción de la investigación científica. El RGPD utiliza un concepto amplio de investigación científica donde se ven integrados componentes tanto públicos (universidades, por ejemplo) como privados.[123] Eso sí, el tratamiento con estos fines no exime a los responsables del tratamiento de tomar medidas suficientes para salvaguardar los derechos y libertades de los individuos, en base al artículo 89 del Reglamento.[124]

La elección de base jurídica condiciona en muchos sentidos a los investigadores. El Reglamento favorece aún más a la excepción de la investigación científica, al conceder varios privilegios a aquellos que se decanten por ella. Aparte de liberar de las pesadas cargas que comporta recabar el consentimiento, la utilización de la excepción científica exime del cumplimiento de los derechos de acceso, rectificación, limitación del tratamiento, oposición y supresión;[125] en caso de que dichos derechos obstaculicen la consecución de los fines de la investigación. También queda limitado el derecho de información del sujeto, siempre que "la comunicación de dicha información resulte imposible o suponga un esfuerzo desproporcionado"[126] para los responsables del tratamiento, y se flexibilizan los principios de limitación de la finalidad y limitación del plazo de conservación.[127]

---

121 QUINN, op. cit., p. 1012.

122 GT29. *Guidelines on Consent under Regulation 2016/679*. 17/EN WP259 rev.01 (28-11-2017), p. 28.

123 159º considerando del RGPD.

124 Artículo 89.1 del RGPD.

125 El artículo 89.2 del RGDP exime del cumplimiento de los derechos de acceso, rectificación, oposición y limitación del tratamiento; mientras que el artículo 17.3 del RGPD exime del cumplimiento de los derechos de supresión y olvido.

126 Artículo 14.5 del RGPD.

127 Artículo 5 b) y e) del RGPD.

Lejos de limitar la innovación científica, el Reglamento parece lograr así un equilibrio entre investigación científica y derecho de privacidad, que toma en consideración las preocupaciones que quitaban el sueño a los investigadores.

Sin embargo, la divergencia en la legislación interna de cada uno de los Estados Miembros puede destruir este delicado equilibrio. El Reglamento permite cierto margen de discrecionalidad a los Estados en algunas áreas, y el tratamiento de datos con fines de investigación científica es uno de ellos. La perseguida armonización de las legislaciones en este ámbito parece un objetivo imposible de alcanzar.

A modo de ejemplo, en Irlanda se ha realizado una interpretación tan estricta de estas provisiones que la colaboración con otros Estados Miembros se ve muy dificultada. La Data Protection Act de 2018, exige específicamente el consentimiento explícito del paciente de manera previa al tratamiento y limita considerablemente la excepción de la investigación científica, exigiendo el cumplimiento de requisitos y procedimientos que van mucho más allá del Reglamento.[128]

7.2. ¿Impone una carga demasiado elevada para las empresas?

El RGPD diseña un idílico marco jurídico de la protección que datos, que en teoría ha de ser beneficioso para todos los sujetos que se ven involucrados, tanto usuarios como empresas. Desde la perspectiva de estas últimas, la adhesión al Reglamento podría constituir una ventaja competitiva.

Pero como suele decirse, "del dicho al hecho, hay un trecho". La realidad es que las empresas se enfrentan a grandes desafíos en la implementación de las novedades propuestas por el GDPR.

En primer lugar, es evidente que la nueva regulación supone un fuerte desembolso económico para las empresas, en dos sentidos distintos. Por una parte, por la inversión en nuevas tecnologías y servicios, como el uso de técnicas de encriptación, pseudonimización y anonimización o la implantación del concepto de privacidad desde el diseño en productos reales. Por otra parte, las empresas se arriesgan a sanciones de una cuantía mucho más significativa.

[128] DONNELLY, Mary y MCDONAGH, Maeve. "Health research, consent and the GDPR Exemption." *European Journal of Health Law,* núm. 26, 2019, pp. 114-119.

Por ello, muchas empresas perciben el Reglamento como una pesada carga. Un sondeo a nivel europeo reveló antes de la entrada en vigor del RGPD que el 68% de los profesionales que tratan con tecnologías en sus negocios veían los nuevos requisitos como una "carga financiera para su negocio".[129]

Además, el alto nivel de libertad que el Reglamento proporciona a las empresas en el cumplimiento de sus obligaciones presenta como contrapartida la inseguridad y las dificultades interpretativas. ¿Cuáles son los medios más adecuados para su cumplimiento? ¿Cómo pueden estar seguras de haber adoptado las medidas de seguridad adecuadas para evitar ser sancionadas?

Dentro del panorama empresarial, los mayores desafíos a la hora de ponerse al día recaen sobre las PYMES.

Una reciente encuesta realizada por la UE en el 2019 demostró que los pequeños negocios aún están lejos de alcanzar el nivel de seguridad y exigencia que pretende garantizar el Reglamento.[130] La encuesta entrevistó a 716 PYMES distribuidas en todo el territorio de la UE un año después de la entrada en vigor del Reglamento, para llegar a la conclusión de que "las respuestas sugieren una amplia ignorancia acerca de las herramientas de seguridad de datos y débil adherencia a las provisiones de privacidad clave del Reglamento".[131]

En general, el problema no es la ausencia de inversión económica para adaptarse a la legislación; sino la falta de entendimiento de conceptos básicos de la misma.

La encuesta averiguó que el 44% de los negocios fallan o no están seguros acerca del cumplimiento de requisitos como la obtención del consentimiento en los términos que prevé la legislación o la existencia de una base jurídica adecuada para el tratamiento de la información.[132]

Tampoco parece que muchos de estos negocios entiendan conceptos como la "encriptación". A pesar de que dos tercios de los encuestados aseguraron utilizar un cifrado

---

[129] ROSSI, Ben. "77% of UK businesses say EU's new data law is a financial burden". (*Information Age*, 29-09-2015). Disponible en: <http://www.information-age.com/77-uk-businesses-sayeus-new-data-law-financial-burden-123460254/> [Consulta: 24-2-2020].

[130] GDPR.EU. "Millions of small businesses aren't GDPR compliant, our survey finds". (*GDPR.EU*, 2019). Disponible en: <https://gdpr.eu/2019-small-business-survey/> [Consulta: 24-2-2020].

[131] Ibid.

[132] Ibid.

end-to-end en su *email*, solo el 9% identificó servidores que realmente ofrecían este servicio.[133] Otra facción relevante de los negocios encuestados, el 22%, confesó no hacer uso de medidas técnicas para la protección de los datos personales.[134]

La situación es complicada. Las pequeñas empresas no tienen medios con los que plantar cara a todos estos cambios, ni recursos económicos para hacer frente a una sanción de la cuantía que plantea el Reglamento. Frente a las PYMES, las grandes multinacionales se encuentran en una posición mucho más favorable.

Uno de los objetivos de la Unión Europea en el desarrollo del Reglamento era equilibrar el campo de juego entre las empresas norteamericanas y las empresas europeas. Sin embargo, el tejido empresarial europeo está compuesto a base de PYMES, mientras que la gran mayoría de las multinacionales proceden de Estados Unidos.

Las exigencias del Reglamento podrían llevar a muchas PYMES a recurrir a las grandes multinacionales, que cuentan con muchas más facilidades para el cumplimiento de los requisitos de protección de datos, como proveedoras de bases de datos o servicios en la *Nube*.[135]

¿Supondrían estas limitaciones una desventaja competitiva para las empresas europeas frente a las grandes multinacionales americanas?

Desde esta perspectiva, la lógica de la legislación europea podría volverse en su contra, y dar como resultado el efecto contrario al pretendido en primera instancia.

7.3. ¿Es adecuado el actual sistema del consentimiento informado?

¿Es el consentimiento que otorgamos realmente libre e informado? ¿Son las políticas de privacidad la solución más adecuada para garantizar el control de los individuos sobre sus datos?

---

[133] Ibid.

[134] Ibid.

[135] SIRUR, Sean; NURSE, Jason y WEBB, Helena. "Are we there yet? Understanding the challenges faced in complying with the General Data Protection Regulation (GDPR)". *MPS '18: Proceedings of the 2nd International Workshop on Multimedia Privacy and Security,* 2018*,* p. 94.

Algunos autores han venido a poner en tela de juicio las bases de la protección de datos en Europa, haciendo referencia a la denominada "paradoja de la privacidad".[136] Su explicación es sencilla.

Los individuos aseguran valorar su privacidad, y exigen tener el control sobre sus datos en todo momento. Encuestas públicas realizadas en Estados Unidos y Reino Unido demuestran respectivamente que el 86% y el 88% de los participantes valoran su privacidad y toman medidas para protegerla.[137] En la práctica, los consumidores muestran una gran indiferencia e ignorancia hacia la privacidad. Los individuos tendemos a compartir grandes cantidades de información a través de Internet, sin preocuparnos apenas de las consecuencias que pueda traer para nuestra privacidad. Un estudio demostró en 2016 que, aunque dos de cada tres individuos decían valorar su privacidad, solo 1 de cada 10 utilizaba técnicas de encriptación en su email.[138]

En otras palabras, la paradoja de la privacidad hace referencia a la discordancia entre nuestra forma de hablar y actuar en relación a la protección de nuestros datos.

El RGPD desarrolla un esquema de protección de datos que se vertebra alrededor del consentimiento del individuo. Las empresas que actúan *online* canalizan las exigencias del Reglamento en relación al consentimiento a través de las "políticas privacidad". Cuando pensamos en una de estas políticas, se nos vienen a la cabeza larguísimos textos técnicos en letra pequeña, que introducen conceptos que ni entendemos ni queremos entender. Al final de estos textos suele haber una casilla que nos solicita consentir a la política de privacidad de la empresa.

El Reglamento ha tratado de clarificar estos incomprensibles textos a través del principio de transparencia, que exige la redacción en un lenguaje claro y sencillo. Sin embargo, esto no pone fin a la problemática.

Puede que los términos de las políticas de privacidad sean accesibles para todo el mundo; pero no por ello dejan de reflejar la tiranía de las grandes multinacionales. *Facebook*, *WhatsApp*

---

136 WILLIAMS Meredydd; NURSE, Jason y CREESE, Sadie. "Privacy is the boring bit: user perceptions and behaviour in the Internet-of-Things." *15th Annual Conference on Privacy, Security and Trust,* 2017, pp. 181-190 y WILLIAMS, Meredydd; NURSE, Jason R.C and CREESE, Sadie, "The perfect storm: the privacy paradox and the Internet-of-Things." *11th International Conference on Availability, Reliability and Security,* 2016, pp. 644-652.

137 WILLIAMS, "Privacy is the boring bit…", cit., pp. 181-182.

138 WILLIAMS, "The perfect storm…", cit., p. 645.

o *Google*, son algunos de los ejemplos más evidentes de grandes empresas que imponen sus políticas de privacidad *online* a los usuarios. La solución es fácil: si no aceptas sus términos y condiciones, puedes buscar una alternativa.

Pero, ¿quién se molesta en encontrar un buscador de Internet alternativo a *Google* cuya política de privacidad sea más favorable al usuario? ¿A qué otras redes sociales podemos acudir si todos nuestros amigos ya son miembros de *Facebook*? O ¿Cómo nos comunicaremos si nuestros contactos ya hacen uso de *WhatsApp*?

La desconfianza acerca de la eficacia de un sistema que gira en torno al consentimiento informado han llevado a la consideración de otras alternativas que proponen reducir (que no eliminar) el peso del consentimiento informado en favor de la responsabilidad de las empresas.

En 2012, *Microsoft* organizó una serie de conferencias que reunieron a 78 participantes procedentes de gobiernos, academia y compañías, con la intención de dialogar acerca del papel del consentimiento en la protección de datos y proponer soluciones alternativas.[139] Estas reuniones advocaban hacia la necesidad de trasladar la responsabilidad de los usuarios hacia las empresas.

El sistema ideado estaría basado en la rendición de cuentas por parte de las empresas en lugar del mero cumplimiento de los requisitos normativos.[140] El concepto de privacidad desde el diseño ocuparía un lugar privilegiado en este entramado.

El consentimiento seguiría formando una base jurídica apropiada en circunstancias concretas, en base al tipo de datos que se pretendan tratar, como los datos sensibles, o a los usos de la información obtenida.[141] Seguramente, el individuo prestaría más atención a la hora de dar su consentimiento y se obtendría un verdadero "consentimiento informado".

La alternativa propuesta revertiría el sistema que hasta ahora conocemos, pero merecería la pena explorarla.

8. UN ESTÁNDAR GLOBAL DE PRIVACIDAD

[139] CATE, Fred y MAYER-SCHÖENBERGER, Viktor. "Notice and consent in a world of big data". *International Data Privacy Law,* núm. 3, 2013, p. 68.

[140] GIL, Elena, op. cit., p. 133.

[141] CATE, op. cit., p. 69.

Dos años después de la entrada en vigor del RGPD, podemos ciertamente observar una tendencia global a incrementar los niveles de privacidad y protección de datos, apreciable tanto en gobiernos como en empresas privadas.

Desde un primer momento, la UE se esforzó por diseñar un instrumento jurídico cuya validez fuese más allá de sus fronteras; un referente a nivel mundial que fijase los parámetros de privacidad más exigentes hasta el momento. El carácter extraterritorial al que hemos hecho referencia y las normas que regulan los flujos transfronterizos de datos ilustran esta ambición.

Ciertamente, su validez se ha extendido considerablemente en la práctica hasta el momento. Muchos hablan de una manifestación más de lo que ha venido a denominarse el "efecto Bruselas".[142] El Reglamento se ha convertido en un estándar global de privacidad *de facto*, al que se adhieren administraciones y empresas de cualquier parte del Globo.

8.1. Un estándar aplicable en cualquier rincón del mundo.

El efecto de la nueva normativa no solo alcanza al "mundo occidental", sino que se hace hueco en legislaciones de cualquier parte del mundo.

Dos factores influyen en este hecho. La extraterritorialidad implica que las empresas tendrán que adaptarse al Reglamento cuando sus operaciones de tratamiento de datos afecten a ciudadanos europeos.

Por otro lado, el Reglamento impide las transferencias de datos personales de ciudadanos de la UE a terceros países u organizaciones internacionales salvo que estos garanticen un "nivel de protección adecuado",[143] verificado por la Comisión Europea.[144] En caso contrario, no podrá realizarse la transferencia, a no ser que el tercer país haya ofrecido "garantías adecuadas" y los usuarios cuenten con "derechos exigibles y acciones legales efectivas".[145]

En consecuencia, muchos Gobiernos han visto la oportunidad de adaptar sus legislaciones internas a los requisitos de la UE, con el objetivo de acceder más fácilmente al mercado

---

[142] La profesora Anu Bradford describe el "efecto Bruselas" como el fenómeno de europeización en muchos aspectos del comercio y política global (como protección de datos, protección del consumidor o protección medioambiental), gracias a la promulgación de regulaciones por parte de la UE que son posteriormente adoptadas como estándares internacionales por Estados y empresas. Ver BRADFORD, Anu. *The Brussels Effect-how the European Union Rules de World.* Oxford University Press, 2020.

[143] Artículo 45.1 del RGPD.

[144] Artículo 45.2 del RGPD.

[145] Artículo 46.1 del RGPD.

interior. En Sudáfrica, la Ley de protección de datos aprobada en 2013 fue diseñada a imagen y semejanza de la normativa europea.[146] En julio de 2018, la UE y Japón reconocieron mutuamente la adecuación de sus legislaciones de protección de datos, dando vía libre a los flujos transfronterizos entre ellos. Para conseguir el visto bueno de la Comisión, el gobierno japonés tuvo que implementar medidas de seguridad adicionales que adaptasen su legislación a los estándares europeos.[147]

8.2. Estados Unidos y el RGPD.

Una de las mayores incógnitas sobre la eficacia extraterritorial del RGPD es qué impacto tendrá el Reglamento sobre las normas de protección de datos estadounidenses.

Sin duda alguna, Estados Unidos se encuentra muchos pasos por delante de Europa en la pugna por el liderazgo digital. No hay más que observar de dónde proceden las grandes multinacionales que controlan la mayor parte de los datos de los ciudadanos europeos.

Pese a ello, sus normas no han demostrado estar a la altura de los desafíos que plantea la era digital en el ámbito de la privacidad. El reciente escándalo de *Cambridge Analytica* es una buena prueba de ello.

Cambridge Analytica era una empresa dedicada al análisis de datos para el desarrollo de campañas publicitarias. En 2018, una investigación conjunta de The Observer y The New York Times reveló cómo esta empresa había recabado información personal de más de 50 millones de perfiles de usuarios de *Facebook* sin su consentimiento con la intención de modular el voto e influir en los resultados de las elecciones presidenciales en Estados Unidos.[148]

En el origen del escándalo se encuentra un aparentemente inocente test de personalidad diseñado por Alexander Kogan en 2013, que accedió a *Facebook* en calidad de analista académico. Sin ser conscientes de ello, los usuarios que realizaban el test consentían el acceso

---

[146] Cipp Guide. "South Africa's new Privacy Law" (*Cipp Guide*, 2013). Disponible en <https://www.cippguide.org/2013/09/09/south-africas-new-privacy-law/> [Consulta: 5-03-2020].

[147] Skadden. "Data Protection in Japan to align with GDPR". (*Skadden*, 2018). Disponible en <https://www.skadden.com/insights/publications/2018/09/quarterly-insights/data-protection-in-japan-to-align-with-gdpr> [Consulta: 5-03-2020].

[148] El País. "La compañía que burló la intimidad de 50 millones de estadounidenses". (*El País*, 21-03-2018). Disponible en <https://elpais.com/internacional/2018/03/20/estados_unidos/1521574139_109464.html> [Consulta: 05-03-2020].

a sus contactos. Gracias a ello, obtuvo la información de más del 15% de la población de Estados Unidos.[149]

La información recabada a través del test de personalidad fue utilizada para realizar perfiles psicológicos de los usuarios, de manera que cada uno de ellos recibía publicidad personalizada dirigida a modular su voto.

Toda esta trama demostró con qué facilidad las grandes empresas pueden manipular a los usuarios de Internet y la consecuente posición de vulnerabilidad en la que estos se encuentran.

La escalofriante noticia fue objeto de comentarios en todas partes del mundo, y con ello las críticas hacia la ineficacia de las normas de protección de datos estadounidenses se multiplicaron.

En este contexto, la comparativa entre la protección de datos europea y norteamericana se hace inevitable. Hemos de comenzar recalcando que estos sistemas son completamente diferentes. Tradicionalmente, el sistema de protección de datos americano ha optado por adoptar unos estándares de privacidad mucho más laxos. De hecho, la Constitución Americana ni siquiera reconoce a sus ciudadanos un derecho fundamental a la privacidad.[150]

En lugar de diseñar un instrumento jurídico a nivel federal que establezca un marco jurídico de protección de datos único aplicable en todo su territorio, el Derecho de protección de datos americano se compone de un entramado de normas sectoriales, que regulan la utilización de la información de los individuos en distintas áreas de actuación, como el sanitario o el sector financiero.[151] Cada una de estas normas tiene un ámbito de aplicación muy limitado, y proporciona su definición particular de conceptos como datos de carácter personal o violación de la seguridad.

---

[149] BBC. "5 claves para entender el escándalo de Cambridge Analytica que hizo que Facebook perdiera US$37.000 millones en un día". (*BBC*, 21-03-2018). Disponible en <https://www.bbc.com/mundo/noticias-43472797> [Consulta: 05-03-2020].

[150] VOSS, Gregory y HOUSER, Kimberly A. "Personal data and the GDPR: providing a competitive advantage for U.S. companies", *American Business Law Journal,* vol. 56, núm.2, p. 295.

[151] Algunos ejemplos son la Health Information and Portability Accountability Act of 1996 o la Financial Data under the Gramm-Leach-Bliley Act (GLBA). Ver: BENADY, David. "GDPR: Europe is taking the lead in data protection". (*Raconteur*, 2018). Disponible en <https://www.raconteur.net/hr/gdpr-europe-lead-data-protection>. [Consulta: 05-03-2020].

No hay tampoco norma federal alguna que obligue a los responsables del tratamiento de datos a elaborar políticas de privacidad que informen del uso que estas hacen de los datos de sus usuarios.[152]

A todo lo anterior se añaden las competencias legislativas de los estados. Cada uno de ellos tiene capacidad para diseñar sus propias normas de protección de datos. Es precisamente en este escalón legislativo donde han comenzado a manifestarse ciertas intenciones de aproximación hacia el estándar europeo de protección de datos.

El mejor ejemplo es la reciente California Consumer Privacy Act (CaCPA) de 2018, que muchos han venido a considerar una reproducción del RGPD a pequeña escala.[153] Otros estados, como Arizona o Vermont, también han endurecido significativamente sus normativas de protección de datos.[154]

Además, algunas de las grandes tecnológicas americanas -entre ellas, *Apple* y *Facebook*- tratan de presionar a la Casablanca para desarrollar un marco de protección de datos unificado y coherente similar al de la UE, para facilitar el funcionamiento de aquellas empresas que operan a ambos lados del Atlántico.[155]

8.3. La privacidad como ventaja competitiva.

El modelo americano de protección de datos que acabamos de describir observaba a la privacidad desde la óptica de la libertad; mientras que el europeo emana un carácter profundamente proteccionista.

Los americanos consideraban a los estándares de privacidad de la UE como una traba al libre funcionamiento del mercado; un obstáculo que reducía la fuerza competitiva de sus empresas.

Pero lo que antes constituía una debilidad, ahora puede ser aprovechado como una ventaja competitiva. Aparte de los gobiernos, las empresas de todo el mundo también han colocado la privacidad entre sus prioridades.

---

[152] VOSS, op. cit., p. 301.

[153] REDONDO, Beatriz. "Protección de datos en Estados Unidos: ¿Cómo afecta a tu negocio?". (*Mailjet*, 2019). Disponible en <https://es.mailjet.com/blog/news/noticiasproteccion-de-datos-eeuu/> [Consulta: 08-03-2020].

[154] Ibid.

[155] The Financial Times. "Apple and Facebook call for EU-style privacy laws in US". *(The Financial Times,* 24-10-2018). Disponible en: <https://www.ft.com/content/0ca8466c-d768-11e8-ab8e-6be0dcf18713> [Consulta: 05-03-2020].

En este sentido, las empresas incluirían el cumplimiento de los estándares de privacidad de la norma europea -la más estricta y protectora del consumidor en el plano internacional hasta el momento- como una cualidad más de su producto. La idea es que los consumidores, a la hora de elegir un servicio, valoren no solo el precio, calidad y otras características, sino también el nivel de privacidad que ofrece el proveedor.

Algunas de las mayores tecnológicas a nivel global ya se han decantado a favor de esta tendencia. En concreto, las grandes multinacionales americanas, cuyo nivel de credibilidad ha disminuido considerablemente después del escándalo de *Cambridge Analytica*, se han sumado a esta pugna. En esta línea, *Facebook*[156] y *Google*[157] han declarado su firme compromiso de cumplir a rajatabla con las exigencias de la legislación.

Microsoft anunció que proporcionaría el nivel de privacidad exigido por el RGPD a todos sus consumidores, independientemente de su lugar de residencia.[158]

Otras empresas podrían seguir el ejemplo de *Microsoft*. El ofrecimiento del más alto estándar de privacidad a todos sus consumidores no solo supone un valor añadido para sus servicios, sino que además facilitaría la operatividad de las compañías y reduciría los costes de cumplimiento al no tener que adaptarse a cada una de las normativas de privacidad alrededor del mundo.

Aunque la realidad de las empresas podría diferir de sus declaraciones. De hecho, *Google* se ha convertido en la primera gran empresa en ser multada por incumplimiento del RGPD. La CNIL, autoridad francesa de la protección de datos, ha impuesto recientemente una multa de más de 50 millones de euros, por incumplir el principio de transparencia, al no proporcionar información adecuada a los usuarios y no obtener un consentimiento válido que permita tratar sus datos con el objetivo de personalizar su publicidad.[159]

---

156 Facebook. "Compromiso de Facebook con la protección de datos y la privacidad de conformidad con el RGPD*"*. (*Facebook*, 29-01-2018). Disponible en: <https://www.facebook.com/business/news/facebooks-commitment-to-data-protection-and-privacy-in-compliance-with-the-gdpr> [Consulta: 26-2-2020].

157 MALCOLM, William. "Our preparations for Europe's new data protection law". (*Google*, 11-05-2018). Disponible en: <https://www.blog.google/topics/public-policy/our-preparations-europes-new-data-protection-law/> [Consulta: 26-2-2020].

158 BRILL, Julie. "Microsoft's commitment to GDPR, privacy and putting customers in control of their own data". (*Microsoft*, 21-05-2018). Disponible en <https://blogs.microsoft.com/on-the-issues/2018/05/21/microsofts-commitment-to-gdpr-privacy-and-putting-customers-in-control-of-their-own-data/> [Consulta: 26-2-2020].

159 "Google is first company hit with major GDPR fine". *Computer fraud & security,* vol. 2019, núm. 2, 2019, p.3.

9. RECOMENDACIONES

Llegados a este punto, deberíamos tener una idea más o menos clara del panorama de la protección de datos en Europa, liderado por el RGPD, con todas sus virtudes y defectos. Es el momento de atrevernos a lanzar algunas conclusiones, alternativas y recomendaciones para la mejora de este sistema.

9.1. Facilitar la investigación científica en el marco de la protección de datos.

La UE reconoce un alto valor a la investigación científica, siendo la creación de un "Espacio Europeo de Investigación" un objetivo reconocido por el artículo 179 del TFUE. La Unión fomenta las acciones de reutilizar y compartir información científica, como demuestran los proyectos OpenAIRE (Open Access Infraestructure for Research in Europe) o la Nube Europea de la Ciencia Abierta.[160]

El reciente Reglamento podría considerarse "amigo" de la investigación científica, pues dota a los investigadores de un cierto margen de libertad del que no gozan otros responsables del tratamiento de datos.

Dicho lo anterior, el RGPD deja no pocas cuestiones abiertas que deberían ser abordadas.

En lo que respecta al consentimiento, parecería adecuado integrar el 33º considerando (referido al consentimiento genérico) en el articulado del Reglamento en sí, para aclarar cómo se relacionaría y cómo flexibilizaría los requisitos del consentimiento informado habitual. Así los investigadores sabrían a qué han de atenerse en caso de optar por el consentimiento como base jurídica en sus investigaciones.

Igualmente, sería interesante hacer referencia a otras modalidades de consentimiento a las que actualmente se recurre en el campo de la investigación científica, como el "consentimiento diferenciado" (*tiered-consent*) o el "consentimiento dinámico" (*dynamic consent*).[161] Ambas parecen ser alternativas adecuadas para compatibilizar consentimiento genérico y control de los individuos sobre sus datos.

---

[160] Supervisor Europeo de Protección de Datos (SEPD). *A preliminary opinion on data protection and scientific research* (2020), p. 12.

[161] En un sistema de *tiered-consent*, el individuo tiene la posibilidad de dar un consentimiento genérico exclusivamente para determinados tipos de investigación o usos (por ejemplo, limitado a un tipo de enfermedades). En un sistema de *dynamic-consent* los individuos irían proporcionando su consentimiento para determinadas actividades a lo largo del tiempo de manera digital. Ver: SEPD, op. cit., p. 14.

Por otro lado, parecería oportuno especificar qué se entiende por "medidas de salvaguarda" en el artículo 89 (aparte de la pseudonimización de los datos). Por ejemplo, el consentimiento informado de los participantes en la investigación, sin constituir la base jurídica para el tratamiento de datos, podría constituir una medida de salvaguarda eficaz.[162] Esta medida podría satisfacerse precisamente a través de las formas de consentimiento que acabamos de mencionar. La adhesión a códigos de conducta y la supervisión y obtención de certificados por parte de Comités Éticos serían otras opciones igualmente eficaces.[163]

Por último, las divergencias entre las normativas internas de cada uno de ellos podrían dañar la ambición de un Espacio Europeo de Investigación que fomente la reutilización de datos y la conducción de investigaciones científicas interestatales. Ya hemos resaltado la magnitud de este problema. Por ello, es necesario garantizar un mayor nivel de armonización entre las legislaciones de los Estados Miembros.

9.2. "Empoderar" al individuo en el ejercicio de sus derechos.

En los últimos años se han desarrollado algunas iniciativas que abogan por un verdadero sistema de empoderamiento del individuo. En este sistema, el individuo ha de ser plenamente consciente del uso que las empresas hacen de sus datos, para poder tomar decisiones realmente informadas y aprovecharse del potencial que ofrecen sus datos. Una de las iniciativas más prometedoras es *MyData.*[164]

Para garantizar su éxito, el sistema debería virar desde la "protección de datos" hacia el "empoderamiento de los datos".[165] En lugar de tratar de proteger al individuo frente a los abusos que las empresas cometen con sus datos, se trataría de facultarle para utilizar sus datos en su propio beneficio.

Pese a que el RGPD reconoce poderosas armas a disposición de los individuos, la ausencia de correspondientes herramientas técnicas y estándares hace que estos derechos sean en la práctica muy difíciles de ejercitar.[166] Debería realizarse un esfuerzo para transformar estos derechos "formales" en derechos realmente "accionables".

---

[162] SEPD, op. cit., p. 20.

[163]MAHSA, Shabani. "Rules for processing genetic data for research purposes in view of the new EU General Data Protection Regulation". *European Journal of Human Genetics,* núm. 26*,* 2018, pp. 149-156.

[164] Ver: MyData, *Declaration of MyData Principles*. Disponible en <https://mydata.org/declaration/> [Consulta: 13-04-2020].

[165]Ibid, principio 1.2.

[166] Comisión Europea, *A European Strategy*… cit., p. 10.

El derecho a la portabilidad de los datos tiene un gran potencial en este sentido, pero presenta dificultades de aplicación práctica. Los usuarios deberían estar habilitados para hacer efectivo este derecho, teniendo la posibilidad de descargar la información personal que quieren dejar de compartir en un servicio y trasladándolo a otro.

Por otro lado, los individuos deben ser capaces de entender las políticas de privacidad y manejarlas a su disposición, dando y retirando su consentimiento a voluntad.[167] Además, los términos y condiciones de las políticas de privacidad -que ahora son unilateralmente diseñados por las empresas dedicadas al tratamiento de los datos- deberían ser negociables de forma justa con los individuos.

Aparte del reconocimiento y esfuerzo legal por adaptarse a estos principios, este sistema requeriría del diseño de aplicaciones y herramientas que faciliten el manejo de la información personal y el consentimiento.[168] Incluso se han desarrollado algoritmos que permiten a los usuarios de Internet controlar los datos que están facilitando y monetizarlos; es decir, cobrar por la venta de sus datos a los buscadores de Internet.[169]

Si bien este sistema parece utópico a día de hoy, puede hacerse realizable en un futuro no tan lejano. Para el desarrollo de todo su potencial, una legislación acorde a sus principios sería un primer paso.

9.3. Integrar a las PYMES en la protección y economía de los datos.

Las pequeñas y medianas empresas ocupan el 99% del tejido empresarial en la UE, implicando a más de 23 millones de negocios.[170] Es decir, las PYMES constituyen el principal motor económico de la UE.

Por ello, es vital que las PYMES no perciban al Reglamento como un enemigo, sino como una oportunidad para su negocio.

En esta tarea, las Administraciones Públicas deben colaborar mano a mano con las empresas. Primero, han de facilitarse no solo guías teóricas, sino también el soporte técnico necesario para garantizar el cumplimiento con la normativa. Asimismo, pueden desarrollarse

---

[167] MyData, op. cit., principio 3.4.

[168] Comisión Europea, *A European Strategy*… cit., p. 10.

[169] Se trata de la aplicación Pay-per-track, diseñada en 2017 por un investigador de la Universitat Rovira i Virgili (URV). Ver: La Razón. "Cobrar por mis datos personales". (*La Razón*, 7-09-2017). Disponible en <https://www.larazon.es/tecnologia/cobrar-por-mis-datos-personales-BO15937314/> [Consulta: 13-04-2020].

[170] GDPR.EU. "Millions of small businesses…", cit.

aplicaciones permanentes que permitan a una empresa autoevaluar su nivel de cumplimiento.[171]

Más allá del cumplimiento de la normativa, ha de realizarse un esfuerzo por hacer comprender a los empresarios el valor de la digitalización y el *big data* y ayudarles a sacar el máximo provecho de todas sus posibilidades. Para ello, sería conveniente fomentar programas de entrenamiento y educación digital para PYMES.

9.4. Incrementar el nivel de armonización entre Estados Miembros.

Uno de los objetivos básicos del Reglamento es crear un marco jurídico homogéneo de protección de datos en el marco de la UE sobre el cual pueda asentarse un Espacio Europeo de Datos. Dentro de este, se habilitarían espacios específicos para sectores estratégicos, como sanitario, científico, industrial, financiero, de transporte, etc.[172]

Uno de los peligros que amenazan el desarrollo de este proyecto es la fragmentación existente entre las legislaciones internas de los Estados Miembros. Algunos países -concretamente, Eslovenia, Grecia y Portugal- todavía no han adaptado sus legislaciones al RGPD.[173] Además, hemos visto que el amplio margen de apreciación en relación a la categoría de datos sensibles puede limitar la libre circulación de datos en la UE.

Sería conveniente elaborar normativa sectorial (o adaptar la normativa existente) que aplique los principios de la protección de datos a los ámbitos estratégicos mencionados. Además, este Espacio Europeo de Datos debería ir acompañado por un marco legislativo adecuado que habilite y establezca las bases de su funcionamiento.[174]

Además, la UE debería promover y establecer pautas que faciliten la cooperación entre autoridades de protección de datos de los distintos países de la UE.

9.5. Redefinir el concepto de "datos de carácter personal".

El RGPD limita su ámbito material de aplicación a los datos de carácter personal, definidos por ser aquellos que corresponden a una persona física identificada o identificable.

---

[171] Con la entrada en vigor del RGPD, se diseñó el proyecto SMOOTH, dirigido a facilitar el cumplimiento normativo a las micro-empresas. Sin embargo, este proyecto tiene una fecha caducidad limitada, ya que expira este 2020. Para más información ver: < https://smoothplatform.eu/>.

[172] Comisión Europea, *A European Strategy*… cit., pp. 22-23.

[173] GDPR.EU. "How the GDPR could change in 2020". (*GDPR.EU*, 2019). Disponible en <https://gdpr.eu/gdpr-in-2020/> [Consula: 10-04-2020].

[174] Comisión Europea, *A European Strategy*… cit., p. 12.

Los datos de carácter no personal, donde se incluyen los datos anónimos y los datos proporcionados por terceras personas, quedarían excluidos.

En la práctica, tan drástica distinción no parece eficiente. Y es que a partir de datos anónimos, datos proporcionados por terceras personas y otros tipos de datos de carácter no personal pueden extraerse decisiones o "inferencias" con consecuencias perjudiciales para la privacidad y otros derechos de los individuos.[175]

El GT29, por su parte, ha adoptado una definición más apropiada de datos de carácter personal, diferenciando entre aquellos obtenidos o proporcionados por el individuo, y aquellos inferidos o derivados.[176] En la última categoría se incluirían datos que ahora son considerados de carácter no personal. Esta clasificación adopta una perspectiva teleológica de los datos, enfocada en el resultado obtenido del procesamiento de los datos.

Este encuadre parece más adecuado, y sería apropiado adaptar la legislación existente a tal criterio.

9.6. Adoptar una perspectiva teleológica de la protección de datos.

El RGPD crea una serie de derechos y mecanismos cuyo objetivo es garantizar un control del individuo sobre los datos que proporciona a las empresas. No obstante, apenas fija su atención en el resultado del procesamiento de los mismos, cual son las inferencias o decisiones a las que acabamos de referirnos.

En realidad, el potencial dañino de los datos no se encuentra en su recogida, sino en el uso que pueda hacerse de los mismos. A través de herramientas de *big data analytics*, las empresas son capaces de predecir más cosas de las que somos capaces de imaginar, como nuestras aficiones o preferencias, orientación sexual u opinión política.[177] Estas conclusiones son utilizadas de manera oscura y poco transparente por las empresas; y constituyen la causa de grandes escándalos de privacidad, como el de *Cambridge Analytica*.

El único reconocimiento individual frente a estas prácticas queda recogido en el artículo 22, que protege frente a la toma de decisiones con efectos jurídicos en el individuo basadas exclusivamente en el tratamiento automatizado de datos. Esta protección es claramente insuficiente.

---

[175] WACHTER, Sandra y MITTELSTADT, Brent. "A right to reasonable inferences: re-thinking data-protection law in the age of Big Data and AI". *Columbia Business Law Review,* núm. 2019, 2019, p. 85.

[176] GT29. *Opinion 03/2013 on Purpose Limitation.* 00569/13/EN WP203 (2-04-2013), pp. 46-47.

[177] WACHTER, op. cit., pp. 13-14.

Sería recomendable enfatizar en el resultado del tratamiento de los datos de manera sistemática a lo largo de todo el articulado, empezando por la redefinición del concepto de "datos de carácter personal", como hemos argumentado unas líneas más arriba. Partiendo de este concepto, todos los derechos ya reconocidos por el RGPD se extenderían a los resultados del procesamiento de los datos.

Asimismo, nuevos derechos deberían crearse para complementar la protección que ofrecen los ya existentes. Hay quien apunta a la necesidad de un "derecho a las inferencias razonables".[178] Se trataría de un mecanismo de reacción frente a aquellas "inferencias de alto riesgo" -por estar basadas en fuentes no verificables o poco fiables o implicar riesgo para la privacidad o reputación de los individuos-,[179] que quedan excluidas del ámbito de aplicación del artículo 22.

9.7. Clarificar conceptos jurídicos indeterminados.

Una de las críticas más generalizadas al RGPD es la vaguedad de su terminología.[180] El Reglamento no duda en utilizar continuamente términos como "esfuerzos razonables", "sin dilaciones" o "medidas razonables". Hemos visto esta falta de precisión en distintos momentos a lo largo de todo este Trabajo, sobre todo en el área de las responsabilidades de las empresas. Por ejemplo, la obligación de notificación y comunicación ante una violación de la seguridad nacía cuando dicha brecha causaba un "riesgo" o "alto riesgo" para los derechos y libertades de los individuos;[181] y los conceptos de privacidad desde el diseño y por defecto exigen de la toma de "medidas técnicas y organizativas apropiadas".[182]

¿A qué se refiere el RGPD con todos estos términos? Sin duda, estas ambigüedades crean gran inseguridad jurídica y ansiedad a las empresas encargadas del tratamiento.[183] Un esfuerzo mayor debería dirigirse a aclarar qué se espera de los responsables del tratamiento en cada momento y qué tipo de medidas han de implantar para cumplir con la normativa.

---

[178] Ibid, p. 7.

[179] Ibid.

[180] ABC. "Lo mejor y lo peor de la nueva normativa de privacidad, según los expertos". (*ABC*, 31-05-2018). Disponible en <https://www.abc.es/tecnologia/redes/abci-rgpd-mejor-y-peor-nueva-normativa-privacidad-segun-expertos-201805242219_noticia.html> [Consulta: 10-04-2020].

[181] Artículos 33 y 3 del RGPD.

[182] Artículo 25 del RGPD.

[183] ABC, "Lo mejor y lo peor de la nueva normativa de privacidad…", cit.

10. APÉNDICE: COVID-19 Y BIG DATA

La crisis sanitaria mundial es el escenario propicio para demostrar la repercusión del *big data* en nuestro día a día; así como para poner de manifiesto el delicado equilibrio existente entre análisis de datos masivos y privacidad de los ciudadanos.

El COVID-19 nos proporciona una valiosa muestra de las aplicaciones prácticas del *big data* en el ámbito de la salud pública. Una prueba más de que este fenómeno no es una ilusión; es una realidad que nos afecta ya de pleno, con todas sus bondades y perjuicios.

10.1. Administraciones Públicas y COVID-19.

Las Administraciones Públicas no han tardado en recurrir a las posibilidades del *big data* en sus esfuerzos por controlar la propagación de la pandemia global.

China fue el primero en caer y, consecuentemente, el primero en recurrir a la inteligencia artificial para incrementar la eficacia de las medidas de control de la enfermedad. Las técnicas de *big data* han constituido una pieza central de la estrategia del gigante asiático en la lucha contra el COVID-19, a través del desarrollo de todo un catálogo de aplicaciones móviles que tienen como objetivo último controlar el comportamiento del ciudadano. Una de ellas es capaz de clasificar a las personas en tres colores -verde, amarillo y rojo-, al escanear un código QR personalizado.[184] Este sistema utiliza el GPS del móvil para saber si las personas han estado en una zona de riesgo; y sirve como guía para controlar el movimiento de las personas a pie de calle.[185] En caso de que la persona sea clasificada como "rojo", debe permanecer 14 días aislado en cuarentena.

Estas *apps* han sido tan eficaces como controvertidas. No han sido pocas las voces que se han alzado contra la invasión en la privacidad de los ciudadanos por parte del gobierno chino. Ciertamente, este tipo de medidas -basadas en el uso indiscriminado de datos en poder del gobierno - serían impensables en el territorio de la UE, regido por los principios del RGPD. Sobre todo, si tenemos en cuenta que el *big data* también presenta limitaciones. Un ciudadano chino declaraba que dicha aplicación móvil le clasificaba en color "rojo" injustificadamente,

[184] SÁNCHEZ, Valentina. "China: el código QR para detectar el Covid-19". (*France24*, 2020). Disponible en <https://www.france24.com/es/20200313-china-el-código-qr-para-detectar-el-covid-19> [Consulta: 8-04-2020].

[185] Ibid.

a consecuencia de un viaje en avión que iba a realizar a una zona de riesgo, pero que finalmente canceló.[186]

España -sin llegar tan lejos- se ha sumado también a esta tendencia de aplicación de herramientas basadas en el análisis de datos masivos, como ha plasmado en una Orden Ministerial de 28 de Marzo dirigida a la Secretaría de Estado de Digitalización e Inteligencia Artificial.[187]

En primer lugar, la norma facilita la creación de una aplicación que permita al usuario una autoevaluación en base a sus síntomas, además de proporcionarle información y consejos útiles. El objetivo es incrementar la eficiencia de los servicios sanitarios y la accesibilidad por parte de los ciudadanos.

Sin embargo, lo más llamativo de dicha *app* es que permitirá la "geolocalización del usuario a los solos efectos de verificar que se encuentra en la comunidad autónoma en la que declara estar".[188]

La aplicación ha despertado la polémica, al encontrarse en los difusos límites permitidos por las normas de protección de privacidad de los individuos aplicables (RGPD y LOPD).[189] No obstante, tampoco debemos olvidar que estamos ante una situación excepcional, y la aplicación parece ser de instalación voluntaria. Al instalarla, el usuario conoce estos términos; que, por cierto, no son muy distintos respecto a los de aquellas *apps* que aceptamos sin apenas cuestionarnos (*Google*, *Facebook* y otros muchos servicios que nos piden acceder a nuestra localización).

Si bien parece que la aplicación quedará limitada a verificar la Comunidad Autónoma en la que se encuentra el usuario, la realidad es que fácilmente podría obtenerse un conocimiento mucho más concreto de su posición a través del GPS de su móvil. La clave reside entonces

---

[186] La Vanguardia. "China receta "big data" para controlar a sus ciudadanos y luchar contra el coronavirus". (*La Vanguardia,* 2-03-2020). Disponible en <https://www.lavanguardia.com/vida/20200302/473825002349/china-receta-big-data-control-ciudadano-lucha-coronavirus-inteligencia-artificial-app.html> [Consulta: 08-04-2020].

[187] Orden SND/297/2020, de 27 de marzo, por la que se encomienda a la Secretaría de Estado de Digitalización e Inteligencia Artificial, del Ministerio de Asuntos Económicos y Transformación Digital, el desarrollo de diversas actuaciones para la gestión de la crisis sanitaria ocasionada por el COVID-19.

[188] Ibid.

[189] El País. "Sanidad podrá comprobar mediante su aplicación móvil si un ciudadano está donde declara estar". (*El País*, 6-04-2020). Disponible en <https://elpais.com/economia/2020-04-05/sanidad-podra-comprobar-mediante-su-aplicacion-movil-si-un-ciudadano-esta-donde-declara-estar.html> [Consulta: 8-04-2020].

en que el uso que de dicha información haga el Gobierno se limite al fin que persigue y a lo estrictamente previsto por la norma.

En cualquier caso, nada tiene que ver con el modelo implantado en China, donde la aplicación a la que ya nos hemos referido era de instalación obligatoria para los ciudadanos chinos, y sobrepasaba sonoramente los límites admisibles de intromisión en la intimidad del individuo.

Igualmente polémico es el denominado proyecto "DataCOVID".[190] Hablamos de un estudio de movilidad nacional que permite analizar el cumplimiento de las medidas de distanciamiento social impuestas durante el estado de emergencia sanitaria en el país.[191] El estudio se basa en los datos de más de 40 millones de teléfonos móviles aportados al INE por las tres principales compañías de telefonía móvil en España (*Movistar, Vodafone* y *Orange*).[192] Estos datos se aportan agregados y anonimizados; por lo que quedarían excluidos del ámbito de aplicación del RGPD. En cualquier caso, considerando que su fundamento es el interés y la sanidad pública, el tratamiento de dichos datos podría ampararse en distintas provisiones del RGPD.[193]

El objetivo del análisis de los datos es conocer los patrones de movilidad de los ciudadanos durante la crisis sanitaria para contribuir a la toma de decisiones eficientes en la gestión de la enfermedad.[194] De ninguna manera pueden utilizarse los mismos para usos policiales ni en contra de los ciudadanos individualmente considerados. Con esto se pretende asegurar el respeto a la normativa de protección de datos, tanto española como europea.

10.2. Predicción de la existencia y propagación de la epidemia.

El *big data* no solo facilita a los gobiernos la toma de decisiones relacionadas con la gestión de la pandemia, sino que sus utilidades se remontan a las fases de gestación de la misma.

---

[190] Este proyecto ha tomado como modelo y referente el anterior estudio de movilidad nacional realizado en España el pasado mes noviembre con la colaboración de los mismos operadores (ver apartado 3). Para más información acerca del proyecto DataCOVID, consultar: INE. "Análisis de la movilidad de la población durante el estado de alarma por COVID-19 a partir de la posición de los teléfonos móviles". Disponible en <https://www.ine.es/covid/exp_movilidad_covid_proyecto.pdf> [Consulta: 5-06-2020].

[191] El País. "Más de 40 millones de teléfonos móviles serán usados para rastrear el coronavirus en toda España". (*El País*, 2-02-2020). Disponible en <https://www.abc.es/tecnologia/redes/abci-monitorizara-gobierno-movil-durante-crisis-coronavirus-legal-202003301238_noticia.html> [Consulta: 8-04-2020].

[192] Ibid.

[193] Artículo 6.1.e) y artículo 9.2.i) del RGPD.

[194] El País, *Más de 40 millones de teléfonos móviles*…, cit.

La *start-up* canadiense *BlueDot* pronosticó la existencia de la pandemia el 31 de diciembre de 2019, 10 días antes que la OMS.[195] La empresa utilizó un potente algoritmo que procesa los datos obtenidos de más de 10000 informes (noticias de periódico, comunicados oficiales, páginas web, etc) en 65 idiomas diferentes para anticiparse a los acontecimientos.[196] Eso sí, el capital humano sigue siendo una pieza clave de todo el entramado. Expertos epidemiólogos revisan las conclusiones alcanzadas por el algoritmo para alcanzar correlaciones con sentido desde el punto de vista científico.[197]

Si bien la utilización del *big data* en la predicción de la existencia de enfermedades se ha probado ineficaz en algunas ocasiones, su utilidad es incuestionable en la predicción de propagación de la enfermedad. Por ejemplo, un grupo de investigadores españoles ha diseñado un modelo matemático de expansión del Covid-19 en España a través de un estudio de movilidad de los ciudadanos.[198]

10.3. Nuevos escándalos de privacidad.

El estado de emergencia sanitaria en España -patrocinado por el lema de "quédate en casa"- supone una oportunidad de negocio para aquellas empresas dedicadas al desarrollo de aplicaciones móviles que entretienen a los ciudadanos a falta de otras diversiones.

Entre ellas, *HouseParty* registró un incremento de más de 20 millones de usuarios durante la cuarentena, convirtiéndose en la aplicación más descargada en España en estos tiempos.[199] Sin embargo, su éxito ha sido efímero. La cantidad ingente de datos que recopilan este tipo de aplicaciones es también una mina de oro para los *hackers*. Poco tardó en correr el rumor del robo masivo de datos personales a *HouseParty*, acompañado del abandono histérico de la mayoría de sus usuarios.

---

[195] ASFOURI, Nicolas. "Un algoritmo descubrió el brote de coronavirus antes de que las autoridades lanzaran la alerta". (*ActualidadRT*, 29-01-2020). Disponible en <https://actualidad.rt.com/actualidad/341392-algoritmo-descubrir-brote-coronavirus> [Consulta: 8-04-2020].

[196] BARBIERI, Alberto. "¿Podemos prever una epidemia con "big data"?" (*Nobbot*, 11-03-2020). Disponible en <https://www.nobbot.com/futuro/big-data-coronavirus/> [Consulta: 8-04-2020].

[197] Ibid.

[198] El Confidencial. "Desarrollan un modelo para predecir los sitios de España con más riesgo de Covid-19". (*El Confidencial*, 28-02-2020). Disponible en <https://www.elconfidencial.com/tecnologia/ciencia/2020-02-28/modelo-matematico-predecir-sitios-espana-riesgo-covid_2475320/> [Consulta: 8-04-2020].

[199] ABC. "El miedo a un posible «hackeo» de Houseparty, la aplicación de videollamadas, amenaza con un éxodo de usuarios". (*ABC*, 31-03-2020). Disponible en <https://www.abc.es/tecnologia/redes/abci-miedo-posible-hackeo-houseparty-aplicacion-videollamadas-amenaza-exodo-uusuarios-202003311055_noticia.html#vca=mod-lo-mas-p4&vmc=leido&vso=tecnologia&vli=noticia.foto.tecnologia&vtm_loMas=si> [Consulta: 8-04-2020].

Los dirigentes al mando de la aplicación niegan rotundamente tal acontecimiento, achacándolo a una campaña de desprestigio. Incluso han ofrecido una recompensa de un millón de dólares a aquel que sea capaz de localizar a los responsables de dicha campaña.[200]

En el supuesto de que el *hackeo* sea real, la empresa podría enfrentarse multas millonarias bajo el RGPD, por incumplimiento de sus responsabilidades en caso de violación de la seguridad.[201]

Todos estos ejemplos no son más que las distintas caras de una misma moneda; manifestaciones del impacto del *big data* en la crisis sanitaria global. El *big data* ha influido e influye en todos los estadios de la enfermedad, desde su gestación hasta su propagación y gestión. En lo que a su gestión se refiere, el choque entre privacidad del individuo y otros derechos fundamentales es más evidente que nunca. En este contexto, la polémica se ha generado alrededor del amparo otorgado por las normas de protección de datos (fundamentalmente, el RGPD) y sus límites. ¿Hasta dónde es admisible la intromisión en la privacidad del individuo para proteger la salud pública?

11. CONCLUSIONES

A lo largo de todo este Trabajo hemos comprobado cómo el *big data* puede ser un arma de doble filo. En las manos adecuadas, presenta un inmenso potencial en beneficio de todos. Pero en las manos equivocadas, el *big data* puede derivar en riesgos de equivalente magnitud. Dentro de este catálogo de riesgos, los más palpables son aquellos que chocan con la privacidad del individuo.

Consciente de esta dualidad, la UE ha elaborado una Estrategia de Datos donde el triángulo conformado por *big data*, privacidad y protección de datos ocupa un lugar clave. Sirviéndose del Derecho de protección de datos, se busca alcanzar un equilibrio entre *big data* y privacidad, que garantice al mismo tiempo un adecuado nivel de privacidad de los

[200] El Mundo. "Houseparty niega un hackeo y asegura que se trata de una campaña de desprestigio". (*El Mundo*, 31-03-2020). Disponible en <https://www.elmundo.es/tecnologia/2020/03/31/5e82eda0fdddffc0058b462c.html> [Consulta: 08-04-2020].

[201] El artículo 33 del RGPD obliga a la notificación de las autoridades correspondientes en un plazo de 72 horas desde la brecha de seguridad, y el artículo 34 del RGPD obliga a la comunicación a los ciudadanos afectados en caso de que la violación entrañe un alto riesgo para sus derechos fundamentales.

individuos y un ecosistema de libre circulación de datos acorde con las ambiciosas intenciones europeas (p. ej., Espacio Europeo Datos).

El resultado de estos esfuerzos es el RGPD, el primer instrumento jurídico diseñado para abordar la protección de datos desde la óptica del *big data* y la inteligencia artificial. Con la meta última de alcanzar este equilibrio, el Reglamento refleja distintas pretensiones:

- Empoderar al individuo a través del consentimiento informado y la creación de nuevos derechos.
- Reforzar las obligaciones y responsabilidades de las empresas responsables del tratamiento de datos.
- Reducir la dependencia de las empresas europeas respecto de las grandes multinacionales procedentes de terceros países, gracias a su carácter extraterritorial.
- Incrementar el nivel de armonización entre las legislaciones internas de los Estados Miembros.
- Convertirse en un referente en la protección de datos a nivel mundial.

A día de hoy, ¿hasta qué punto se han satisfecho estas pretensiones?

Comenzando por el final, parece que el Reglamento sí se ha consolidado en cierta medida como un referente en protección de datos a nivel mundial. Prueba de ello es el compromiso adoptado por muchas empresas para adaptarse a sus exigencias en todas sus operaciones, con independencia de la parte del Globo en la que tengan lugar. Incluso ha tenido un significativo eco a nivel estatal. Aunque Estados Unidos, a nivel federal, no parece estar inclinado a tomarlo como referencia; el hecho de que algunos de sus estados, como California, y otros países líderes en tecnología, como Japón, se hayan basado en la normativa europea para el diseño de sus propias legislaciones, refleja esta presencia internacional.

Por el contrario, el RGPD se ha mostrado incapaz de alcanzar el nivel de armonización entre legislaciones internas de los Estados Miembros que pretendía. Este instrumento concede un margen demasiado elevado de discreción en sectores donde se requiere gran homogeneización entre las normativas nacionales, como es el campo de la investigación científica. Iniciativas europeas como el Espacio Europeo de Datos (donde se pretenden habilitar espacios para sectores estratégicos, como el de la investigación científica) no pueden llevarse a cabo si no se salvan estas diferencias entre Estados Miembros.

Tampoco parece que se haya reducido la dependencia de las empresas europeas respecto de las grandes tecnológicas americanas. Ciertamente, la extraterritorialidad del RGPD

equilibra el terreno de juego entre empresas, pues cualquiera de ellas ha de aplicar sus provisiones para tratar los datos de ciudadanos europeos. Sin embargo, las cargas y responsabilidades que diseña el Reglamento resultan especialmente pesadas para las PYMES, aunque relativamente fáciles de soportar para las grandes multinacionales. En muchas ocasiones las PYMES no tienen ni los recursos ni la capacidad tecnológica para implantar o incluso entender las exigencias del Reglamento; y difícilmente pueden hacer frente a las sanciones que implica su incumplimiento. Irónicamente, esto lleva a las pequeñas empresas a depender aún con más fuerza de las grandes multinacionales extranjeras, que se convierten, por ejemplo, en sus proveedoras de servicios en la Nube.

No obstante, la mayor limitación del RGPD reside en lo que podríamos considerar su "columna vertebral": el sistema del consentimiento informado y las políticas de privacidad *online*, su máxima expresión.

El RGPD visualiza un mundo en el que los ciudadanos leen atentamente todos y cada uno de los puntos de las políticas de privacidad y consienten solo cuando están de acuerdo con ellas; están perfectamente informados de sus alternativas y no dudan en hacer uso de sus derechos legales (como la portabilidad de los datos). La realidad, en cambio, es otra muy distinta. La "paradoja de la privacidad" demuestra que los individuos no valoran la privacidad tanto como dicen hacerlo; y las empresas tampoco parecen estar interesadas en que lo hagan.

Ante esta situación, cabrían dos alternativas:

Una primera alternativa consistiría en incrementar la operatividad del sistema en la práctica. Se trataría de garantizar que derechos tan poderosos como la portabilidad de los datos no sean meros reconocimientos vacíos, sino derechos accionables por los individuos. Por otro lado, los usuarios han de tener un papel más activo en la negociación de las políticas de privacidad, y su consentimiento ha de ser verdaderamente libre. Todo ello iría acompañado de aplicaciones y herramientas digitales que faciliten el ejercicio de los derechos y el control de la información personal. Ya dijimos que esta propuesta se encuentra aún en una fase embrionaria, pero quizá no sea tan descabellada en un futuro no tan lejano.

La segunda alternativa sería mucho más radical, pues supondría invertir por completo el esquema que conocemos en dos sentidos:

- Desplazar el centro de gravedad desde el individuo hacia las empresas.
- Adoptar una perspectiva teleológica de los datos.

La normativa se enfocaría en controlar los usos que las empresas hagan de los datos, pues es aquí donde se concentra el verdadero riesgo del *big data*. Es decir, se implantaría un sistema de "rendición de cuentas", en el que las empresas habrían de responder en base al uso que hagan de la información recogida.

Bien es cierto que el RGPD ha incrementado las responsabilidades y cargas de las empresas; pero no por ello ha reducido el peso del consentimiento informado. En este modelo alternativo, el consentimiento quedaría relegado a situaciones específicas, como, por ejemplo, el tratamiento de datos sensibles. Limitando el número de ocasiones en que el individuo ha de prestar su consentimiento, parece más probable que, cuando lo haga, sea efectivamente informado.

Y es que de nada sirve diseñar todo un marco teórico para empoderar individuo, si este es incapaz de utilizarlo en la práctica.

REFERENCIAS BIBLIOGRÁFICAS

LEGISLACIÓN, SENTENCIAS Y CASOS

Carta de Derechos Fundamentales de la UE.

Tratado de Funcionamiento de la Unión Europea.

Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante, "Directiva de Protección de Datos" o "la Directiva").

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

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

Orden SND/297/2020, de 27 de marzo, por la que se encomienda a la Secretaría de Estado de Digitalización e Inteligencia Artificial, del Ministerio de Asuntos Económicos y Transformación Digital, el desarrollo de diversas actuaciones para la gestión de la crisis sanitaria ocasionada por el COVID-19.

Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre de 2000.

Sentencia del Tribunal de Justicia de la UE de 13 de Mayo de 2014, caso C-131/12 *Google Spain SL v. Agencia Española de Protección de Datos*.

Decisión de la CE de 20 de marzo de 2019, caso AT.40411 *Google Search (AdSense)*.

INFORMES Y OPINIONES DE ORGANISMOS DE PROTECCIÓN DE DATOS

Agencia Europea de los Derechos Fundamentales. *Towards more effective policing -Understanding and preventing discriminatory ethnic profiling: a guide.* Oficina de Publicaciones de la Unión Europea, 2010.

Comisión Europea. *A European Strategy for Data.* COM(2020) 66 final (19-02-2020).

GT29. *Working Document on the processing of personal data relating to health in electronic health records (EHR).* 00323/07/EN WP131 (15-02-2007).

GT29. *Opinion 03/2013 on Purpose Limitation.* 00569/13/EN WP203 (2-04-2013).

GT29. *Opinion 05/2014 on Anonymisation techniques.* 0829/14/EN WP216 (10-04-2014).

GT29. *Guidelines for identifying a controller or processor's lead supervisory authority*. 16/EN WP244 (13-12-2016).

GT29. *Guidelines on Consent under Regulation 2016/679*. 17/EN WP259 rev.01 (28-11-2017).

Supervisor Europeo de Protección de Datos (SEPD). *A preliminary opinion on data protection and scientific research* (2020).

LIBROS, ARTÍCULOS Y WEBGRAFÍA

ABC. "El miedo a un posible «hackeo» de Houseparty, la aplicación de videollamadas, amenaza con un éxodo de usuarios". (*ABC*, 31-03-2020). Disponible en <https://www.abc.es/tecnologia/redes/abci-miedo-posible-hackeo-houseparty-aplicacion-videollamadas-amenaza-exodo-uusuarios-202003311055_noticia.html#vca=mod-lo-mas-p4&vmc=leido&vso=tecnologia&vli=noticia.foto.tecnologia&vtm_loMas=si> [Consulta: 8-04-2020].

ABC. "Lo mejor y lo peor de la nueva normativa de privacidad, según los expertos". (*ABC*, 31-05-2018). Disponible en <https://www.abc.es/tecnologia/redes/abci-rgpd-mejor-y-peor-nueva-normativa-privacidad-segun-expertos-201805242219_noticia.html> [Consulta: 10-04-2020].

ALIBEIGI, Ali; MUNIR, Abu Bakar; ERSHADULKARIM, MD y ASEMI, Adeleh. "Towards standard information privacy, innovations of the new General Data Protection Regulation". *Library Philosophy and Practice* (revista electrónica), núm. 2840, 2019.

ÁLVAREZ RIGAUDIA, Cecilia. "Sentencia Google Spain y derecho al olvido". *Actualidad Jurídica Uría Menéndez,* núm. 38, 2014.

ASFOURI, Nicolas. "Un algoritmo descubrió el brote de coronavirus antes de que las autoridades lanzaran la alerta". (*ActualidadRT*, 29-01-2020). Disponible en <https://actualidad.rt.com/actualidad/341392-algoritmo-descubrir-brote-coronavirus> [Consulta: 8-04-2020].

BARBIERI, Alberto. "¿Podemos prever una epidemia con "big data"?" (*Nobbot*, 11-03-2020). Disponible en <https://www.nobbot.com/futuro/big-data-coronavirus/> [Consulta: 8-04-2020].

BBC. "5 claves para entender el escándalo de Cambridge Analytica que hizo que Facebook perdiera US$37.000 millones en un día". (*BBC*, 21-03-2018). Disponible en <https://www.bbc.com/mundo/noticias-43472797> [Consulta: 05-03-2020].

BENADY, David. "GDPR: Europe is taking the lead in data protection". (*Raconteur*, 2018). Disponible en <https://www.raconteur.net/hr/gdpr-europe-lead-data-protection>. [Consulta: 05-03-2020].

BOARDMAN, Ruth; MULLOCK, James y MOLE, Ariane. "Guide to the General Data Protection Regulation". *Bird & Bird*, 2017.

BOURREAU, Marc; DE STREEL, Alexandre y GRAEF, Inge. "Big Data and Competition Policy: market power, personalised pricing and advertising". *Centre on Regulation in Europe,* 2017.

BRADFORD, Anu. *The Brussels Effect-how the European Union Rules de World*. Oxford University Press, 2020.

BRILL, Julie. "Microsoft's commitment to GDPR, privacy and putting customers in control of their own data". (*Microsoft*, 21-05-2018). Disponible en <https://blogs.microsoft.com/on-the-issues/2018/05/21/microsofts-commitment-to-gdpr-privacy-and-putting-customers-in-control-of-their-own-data/> [Consulta: 26-2-2020].

BUDZINSKI, Oliver y STÖHR, Annika. "Competition policy reform in Europe and Germany – institutional change in the light of digitization" *European Competition Journal*, vol. 15, núm. 1, 2019.

CATE, Fred y MAYER-SCHÖENBERGER, Viktor. "Notice and consent in a world of big data". *International Data Privacy Law,* núm. 3, 2013.

Cipp Guide. "South Africa's new Privacy Law" (*Cipp Guide*, 2013). Disponible en <https://www.cippguide.org/2013/09/09/south-africas-new-privacy-law/> [Consulta: 5-03-2020].

Comisión Europea (Comunicado de prensa). "Dar forma al futuro digital de Europa: la Comisión presenta sus estrategias en relación con los datos y la inteligencia artificial". (*Comisión Europea*, 19-02-2020). Disponible en <https://ec.europa.eu/commission/presscorner/detail/es/ip_20_273> [Consulta: 10-04-2020].

Comisión Europea. "¿Qué es el Comité Europeo de Protección de Datos (CEPD)?". (*Comisión Europea*, s.f.). Disponible en <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions/enforcement/what-european-data-protection-board-edpb_es> [Consulta: 23-2-2020].

Comisión Europea. "Questions and Answers-General Data Protection Regulation". (*Comisión Europea*, 2019). Disponible en <https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_387> [Consulta: 16-02-2020].

Comité Europeo de Protección de Datos. "Acerca del CEPD". (*CEPD*, s.f.). Disponible en <https://edpb.europa.eu/about-edpb/about-edpb_es> [Consulta: 8-05-2020].

DE LA TORRE, Tanoj V. "Novedades, cambios y efectos del nuevo RGPD sobre la LOPD". *Inesem* (revista digital), 2017. Disponible en <https://revistadigital.inesem.es/juridico/nuevo-rgpd/>. [Consulta: 25-02-2020].

Deloitte. "GDPR Top Ten #10: One Stop Shop". (*Deloitte*, s.f.). Disponible en <https://www2.deloitte.com/ch/en/pages/risk/articles/gdpr-one-stop-shop.html> [Consulta: 23-2-2020].

Deloitte. "IoT-Internet of Things". (*Deloitte*, s.f.). Disponible en <https://www2.deloitte.com/es/es/pages/technology/articles/IoT-internet-of-things.html> [Consulta: 10-02-2020].

DIKER VANBERG, Aysem y ÜNVER, Mehmet Bilal. "The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo?". *European Journal of Law and Technology,* vol. 8, núm. 1, 2017.

DONNELLY, Mary y MCDONAGH, Maeve. "Health research, consent and the GDPR Exemption." *European Journal of Health Law,* núm. 26, 2019.

El Confidencial. "Alemania inaugura el pulso con EEUU para lograr la "soberanía digital" de la UE". (*El Confidencial,* 17-11-2019). Disponible en <https://www.elconfidencial.com/economia/2019-11-17/alemania-inaugura-el-pulso-con-eeuu-para-lograr-la-soberania-digital-de-la-ue_2339299/> [Consulta: 11-2-2020].

El Confidencial. "Desarrollan un modelo para predecir los sitios de España con más riesgo de Covid-19". (*El Confidencial*, 28-02-2020). Disponible en <https://www.elconfidencial.com/tecnologia/ciencia/2020-02-28/modelo-matematico-predecir-sitios-espana-riesgo-covid_2475320/> [Consulta: 8-04-2020].

El Mundo. "Houseparty niega un hackeo y asegura que se trata de una campaña de desprestigio". (*El Mundo*, 31-03-2020). Disponible en <https://www.elmundo.es/tecnologia/2020/03/31/5e82eda0fdddffc0058b462c.html> [Consulta: 08-04-2020].

El País. "30 millones de datos diarios para conocer al turista". (*El País*, 21-08-2019). Disponible en <https://elpais.com/economia/2019/08/20/actualidad/1566330581_839728.html> [Consulta: 11-2-2020].

El País. "El INE seguirá la pista de los móviles de toda España durante ocho días". (*El País*, 29-10-2019). Disponible en <https://elpais.com/economia/2019/10/28/actualidad/1572295148_688318.html> [Consulta: 11-2-2020].

El País. "Europa ultima un plan para dar la batalla en el negocio de los datos". (*El País*, 17-11-2019). Disponible en

<https://elpais.com/economia/2019/11/16/actualidad/1573926886_318836.html> [Consulta: 11-02-2020].

El País. "La compañía que burló la intimidad de 50 millones de estadounidenses". (*El País*, 21-03-2018). Disponible en <https://elpais.com/internacional/2018/03/20/estados_unidos/1521574139_109464.html> [Consulta: 05-03-2020].

El País. "Más de 40 millones de teléfonos móviles serán usados para rastrear el coronavirus en toda España". (*El País*, 2-02-2020). Disponible en <https://www.abc.es/tecnologia/redes/abci-monitorizara-gobierno-movil-durante-crisis-coronavirus-legal-202003301238_noticia.html> [Consulta: 8-04-2020].

El País. "Sanidad podrá comprobar mediante su aplicación móvil si un ciudadano está donde declara estar". (*El País*, 6-04-2020). Disponible en <https://elpais.com/economia/2020-04-05/sanidad-podra-comprobar-mediante-su-aplicacion-movil-si-un-ciudadano-esta-donde-declara-estar.html> [Consulta: 8-04-2020].

EVANS, David. "The antitrust economics of two-sided markets". *American Enterprise Institute*, 2002, p. 43. Disponible en <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=332022>, [Consulta: 11/02/2020].

Facebook. "Compromiso de Facebook con la protección de datos y la privacidad de conformidad con el RGPD". (*Facebook*, 29-01-2018). Disponible en: <https://www.facebook.com/business/news/facebooks-commitment-to-data-protection-and-privacy-in-compliance-with-the-gdpr> [Consulta: 26-2-2020].

GDPR.EU. "How the GDPR could change in 2020". (*GDPR.EU*, 2019). Disponible en <https://gdpr.eu/gdpr-in-2020/> [Consula: 10-04-2020].

GDPR.EU. "Millions of small businesses aren't GDPR compliant, our survey finds". (*GDPR.EU*, 2019). Disponible en: <https://gdpr.eu/2019-small-business-survey/> [Consulta: 24-2-2020].

GDPR-info. "GDPR-consent". (*GDPR-info*, s.f.). Disponible en <https://gdpr-info.eu/issues/consent/> [Consulta: 18-2-2020].

GIL, Elena. "*Big data*, privacidad y protección de datos". *Agencia Española de Protección de Datos*, 2015. Disponible en <https://www.aepd.es/sites/default/files/2019-10/big-data.pdf>.

"Google is first company hit with major GDPR fine". *Computer fraud & security,* vol. 2019, núm. 2, 2019.

HERRERO SUÁREZ, Carmen. "La economía de los grandes datos o Big Data desde el Derecho de la competencia: ¿nuevos problemas? ¿nuevas soluciones?". *Revista de Derecho de la Competencia y de la Distribución,* núm. 23, 2018.

INE. "Análisis de la movilidad de la población durante el estado de alarma por COVID-19 a partir de la posición de los teléfonos móviles". Disponible en <https://www.ine.es/covid/exp_movilidad_covid_proyecto.pdf> [Consulta: 5-06-2020].

KERBER, Wolfgang. "Digital markets, data, and privacy: competition law, consumer law and data protection". *Journal of Intellectual Property Law & Practice,* vol. 11, núm. 11, 2016.

La Razón. "Cobrar por mis datos personales". (*La Razón*, 7-09-2017). Disponible en <https://www.larazon.es/tecnologia/cobrar-por-mis-datos-personales-BO15937314/> [Consulta: 13-04-2020].

La Vanguardia. "China receta "big data" para controlar a sus ciudadanos y luchar contra el coronavirus". (*La Vanguardia,* 2-03-2020). Disponible en <https://www.lavanguardia.com/vida/20200302/473825002349/china-receta-big-data-control-ciudadano-lucha-coronavirus-inteligencia-artificial-app.html> [Consulta: 08-04-2020].

LOZANO GARROTE, Juan. "Derecho al olvido. La protección de datos frente a los motores de búsqueda como Google". (*Noticias Jurídicas*, 26-04-2019). Disponible en <http://noticias.juridicas.com/conocimiento/articulos-doctrinales/13910-derecho-al-olvido-la-proteccion-de-datos-frente-a-los-motores-de-busqueda-como-google/> [Consulta: 16-02-2020].

MAHSA, Shabani. "Rules for processing genetic data for research purposes in view of the new EU General Data Protection Regulation". *European Journal of Human Genetics,* núm. 26*,* 2018.

MALCOLM, William. "Our preparations for Europe's new data protection law". (*Google*, 11-05-2018). Disponible en: <https://www.blog.google/topics/public-policy/our-preparations-europes-new-data-protection-law/> [Consulta: 26-2-2020].

MAYER-SCHÖNBERGER, Viktor y CUKIER, Kenneth. *Big Data: la revolución de los datos masivos.* Turner Noema, 2013.

MyData, *Declaration of MyData Principles.* Disponible en <https://mydata.org/declaration/> [Consulta: 13-04-2020].

PLATH, Sylvia. "And I sit here without identity: faceless. My head aches" (*PwC Luxembourg*, 2016). Disponible en <https://www.pwc.lu/en/general-data-protection/docs/pwc-anonymisation-and-pseudonymisation.pdf> [Consulta: 17-2-2020].

QUINN, Paul y QUINN, Liam. "Big genetic data and its big data protection challenges." *Computer Law and Security Review,* vol. 34, núm.5, 2018.

REDONDO, Beatriz. "Protección de datos en Estados Unidos: ¿Cómo afecta a tu negocio?". (*Mailjet*, 2019). Disponible en <https://es.mailjet.com/blog/news/noticiasproteccion-de-datos-eeuu/> [Consulta: 08-03-2020].

ROSSI, Ben. "77% of UK businesses say EU's new data law is a financial burden". (*Information Age*, 29-09-2015). Disponible en: <http://www.information-age.com/77-uk-businesses-sayeus-new-data-law-financial-burden-123460254/> [Consulta: 24-2-2020].

SÁNCHEZ, Valentina. "China: el código QR para detectar el Covid-19". (*France24*, 2020). Disponible en <https://www.france24.com/es/20200313-china-el-código-qr-para-detectar-el-covid-19> [Consulta: 8-04-2020].

Signaturit. "GDPR: ¿qué necesitas saber del nuevo Reglamento Europeo de Protección de Datos?" (*Signaturit*, 2018). Disponible en <https://blog.signaturit.com/es/las-claves-sobre-el-nuevo-reglamento-europeo-de-proteccion-de-datos> [Consulta: 18-2-2020].

SIRUR, Sean; NURSE, Jason y WEBB, Helena. "Are we there yet? Understanding the challenges faced in complying with the General Data Protection Regulation (GDPR)". *MPS '18: Proceedings of the 2nd International Workshop on Multimedia Privacy and Security,* 2018.

Skadden. "Data Protection in Japan to align with GDPR". (*Skadden*, 2018). Disponible en <https://www.skadden.com/insights/publications/2018/09/quarterly-insights/data-protection-in-japan-to-align-with-gdpr> [Consulta: 5-03-2020].

The Financial Times. "Apple and Facebook call for EU-style privacy laws in US". *(The Financial Times,* 24-10-2018). Disponible en: <https://www.ft.com/content/0ca8466c-d768-11e8-ab8e-6be0dcf18713> [Consulta: 05-03-2020].

VOSS, Gregory y HOUSER, Kimberly A. "Personal data and the GDPR: providing a competitive advantage for U.S. companies", *American Business Law Journal,* vol. 56, núm.2.

WACHTER, Sandra y MITTELSTADT, Brent. "A right to reasonable inferences: re-thinking data-protection law in the age of Big Data and AI". *Columbia Business Law Review,* núm. 2019, 2019.

WILLIAMS Meredydd; NURSE, Jason y CREESE, Sadie. "Privacy is the boring bit: user perceptions and behaviour in the Internet-of-Things." *15th Annual Conference on Privacy, Security and Trust,* 2017.

WILLIAMS, Meredydd; NURSE, Jason R.C and CREESE, Sadie, "The perfect storm: the privacy paradox and the Internet-of-Things." *11th International Conference on Availability, Reliability and Security,* 2016.